SUBMISSION No. 101

SUBMITTION TO:

Joint Select Committee on Cyber-Safety

Comments of

THE INTERNET KEEP SAFE COALITION

(iKeepSafe.org)

Sally Linford, VP of Communications
Internet Keep Safe Coalition
1401 K Street, NW
Suite 600
Washington, DC 20005
202.487.7552
sally@ikeepsafe.org

June 24, 2010

EXECUTIVE SUMMARY

iKeepSafe is honored to respond to the Terms of Reference of the Joint Select Committee on Cyber-safety. In these comments, we (I.) highlight current and recent digital citizenship initiatives, including international efforts, (II.) discuss new research on youth risk online, and (III.) identify how stakeholders can support schools and reduce the incidence and effects of cyber-bullying and other cyber threats (education solutions and technology solutions).

I. INTRODUCTION: iKeepSafe promotes digital citizenship through internet safety education, industry partnerships, federal projects, policy outreach, and international efforts.

The Internet Keep Safe Coalition (iKeepSafe) is a private-public partnership of leaders from the Internet industry, the health community, child advocacy organizations, law enforcement, the educational community and policymakers.

iKeepSafe's vision is to have generations of children grow up safely using connected technologies. With this mission, iKeepSafe tracks global trends and issues surrounding Internet-enabled products, and develops positive, forward-looking resources to teach the safe and healthy use of connected technology. iKeepsafe has over 100 Coalition partners including, Governors and First Ladies/Gentlemen (in the US), State Attorneys General, corporate sponsors, associations and specialists, and business partners.[1]

iKeepSafe connects policy leaders and Coalition members to create customized community initiatives to address current safety and security issues. We consult with industry and organizations to develop and distribute Internet education materials within their own markets. We provide a digital library of education content that can be customized and co-branded for distribution by schools, corporations, and government leaders.

A. Internet Safety Education

iKeepSafe produces the Faux Paw the Techno Cat® Internet safety series of children's books and animated DVDs. Through the storybook adventures of Internet safety icon, Faux Paw the Techno Cat®, elementary school children learn:

- Internet safety basics
- How to handle cyber-bullying
- Balancing real life with screen time
- The risks and dangers of illegal downloading

The iKeepSafe.org website reinforces the lessons taught in the books with educational materials, including full curriculum, PowerPoint® presentations, activity sheets, coloring pages, and quizzes, available for free download.[2] The Faux Paw® curriculum is based on research from Harvard's Center on Media and Child Health and created in partnership with the iKeepSafe Global Research Team, Penn State University Department of Education, and the University of Maryland. Faux Paw stories are also available in Arabic, Spanish, French, Mandarin, Cambodian, Vietnamese, Hmong, Tagalog, and other languages.

[1] *See* www.iKeepSafe.org for a full list of Coalition members.
[2] www.ikeepsafe.org

iKeepSafe partnered with WoogiWorld to create the CyberHero program which trains and inspires students to use new media as a positive factor in their lives. The CyberHero program is a "classroom" version of the full Woogi World learning environment, exclusively focused on the CyberHero mission to motivate students to become digitally literate.

B. Industry Partnerships

iKeepSafe has numerous partnerships with industry designed to promote Internet safety and digital citizenship. iKeepSafe's most recent partnership is with Google involving a multi-city Digital Literacy Tour in the US. Since December 2009 and June, 2010, and are planning future events in other cities nationally. The purpose of these events is to help parents, younger students and teens learn how to log on together and develop habits and skills that promote online safety and security. In conjunction with this tour, Google and iKeepSafe created four digital literacy videos, as well as instructor booklets and student handouts.[3] The videos and resources teach kids how to stay safe online and on YouTube, as well as how to recognize and steer clear of cyber tricks.

iKeepSafe has a strong partnership with Symantec, an international leader in online security. An iKeepSafe representative sits on Symantec's Corporate Responsibility Advisory Board and the Norton Online Family Advisory Council to provide guidance on critical safety and citizenship issues. iKeepSafe also produced Symantec's "Connected and Protected Tour" which provided safety and security presentations to parents and children across the US in Boys and Girls Clubs and schools. iKeepSafe has completed similar projects with AT&T, the American School Counselors Association, DARE America, and Optimists.

Finally, through multiple industry and foundation sponsors, iKeepSafe is developing the 2010 Digital Network of Support, which provides training materials for parents, technology teachers, school counselors, administrators, librarians, school nurses, law enforcement, and network administrators. These resources will train all the key players how to respond appropriately to cyber issues for both staff and students. (See section III. Below.)

C. Federal Projects

iKeepSafe has completed numerous projects with federal support. In 2008, we completed a major research project with a grant from the US Department of Justice, Office of Juvenile Justice and Delinquency Prevention (OJJDP) in collaboration with Harvard University's Center on Media and Child Health regarding the effectiveness of online teaching tools for parents. Also, for OJJDP's Project Safe Childhood, iKeepSafe produced the "Know Where They Go" media campaign, which included public service announcements and web resources targeted at parents with digital citizenship messages, including safety, security, and ethics. [4]

In 2009, we produced the Internet Safety Education Program for the Department of Education's Office of Innovation and Improvement. Currently, OJJDP is sponsoring iKeepSafe's Cell Safe Kids™,

[3] Video and curricula available at: http://www.ikeepsafe.org/youtube.html.
[4] http://knowwheretheygo.org/

an education project that uses a virtual world to teach children the safe and healthy use of mobile devices.

D. Policy Outreach

iKeepSafe assists policy leaders with the development and distribution of customized initiatives for Internet safety education in their states. For example, iKeepSafe has teamed with Comcast to provide customized, regional education initiatives with state Attorneys General ("AGs"). AG parent presentations currently run in eight states, online and on Comcast Video on Demand, with more states joining this year.

Consulting with governors and first ladies/gentlemen, iKeepSafe brings safety initiatives to elementary schools in states using the Faux Paw the Techno Cat program and curriculum. iKeepSafe also participates in task forces and working groups to provide reports for policy leaders, both regional and federal, such as the Berkman Center's Internet Safety Technical Task Force and National Telecommunications and Information Administration (NTIA) Online Safety Working Group.

E. International Efforts

As we will see in the statistics in the following section (II.), students in many countries are experiencing similar cyber-events (threats and risk), but various countries and cultures approach these risks in a variety of ways. International initiatives that cultivate idea-sharing across borders, increase the safety net for students and encourage broader thinking.

iKeepSafe has particularly benefited from its relationship with our Australian colleagues on the advisory board of CyberSafe World. In 2007, iKeepSafe president, Marsali Hancock, met Australian cyber-safety expert and founder of CyberSafe World, Robyn Treyvaud. Over the last four years, Robyn has collaborated on many iKeepSafe projects, including the production of the curriculum for the Faux Paw the Techno Cat Series. She sits on iKeepSafe's International Advisory Board. She and Dr. Sophie Reid presented at the Family Online Safety Institute (FOSI) PointSmart.ClickSafe summit in 2008. Likewise, Ms Hancock also sits on CyberSafe World's Advisory Board. In 2006, she presented at a cyber-bullying symposium in Australia where she recommended bringing together a wider net of primary stakeholders (including the public health and education communities) to address critical internet safety issues and methods of effective messaging.

iKeepSafe is also a member of the Cyber Peace Initiative in Egypt with First Lady Suzanne Mubarak to produce digital citizenship content in Arabic for distribution throughout Arab-speaking communities in the Middle East. iKeepSafe was invited by the East-West Institute (EWI) to participate in its First Worldwide Cybersecurity Summit (May 2010), exploring new measures to secure the world's digital infrastructure. As a member of the United Nation's International Telecommunication Union (ITU) Child Online Protection Group (COP), iKeepSafe participated in the ITU working group in Geneva, Switzerland and continues with follow-up meetings.

Working with the Chinese government, iKeepSafe published the last two installments of the Faux Paw the Techno Cat® Internet Safety series in China, producing bilingual editions (Mandarin-English) for distribution in Beijing schools. iKeepSafe education materials have been translated into 11 languages

and are used by Coalition members or schools in many nations. We are convinced that international outreach allows everyone to benefit from the shared wisdom as many cultures concurrently address the complexities of our connected world.

II. ONLINE ENVIRONMENT AND MEDIA USE AMONG YOUTH (RESEARCH)

While iKeepSafe cannot speak specifically to the Australian internet environment for youth, we recommend several studies (some crossing international boarders) that will assist Committee members as they make decisions critical to Australian youth:

"EU Kids Online" identifies five primary risks faced by EU youth online[5]

Noted EU researcher, Sonia Livingstone, has recently produced an in-depth study, detailing the primary risks that youth face through connected technologies. Her work at the London School of Economics and as the Director of *EU Kids Online* is instructive to many in the online education community. Livingstone identifies, "five risks youth face online"[6] in order of likeliness to occur:

1. Giving out personal information, around 50 percent (varying slightly in different countries);
2. Viewing pornography, roughly 40 percent;
3. Seeing violent or hateful content, around 33 percent (roughly 1/3 of teens),
4. Cyberbullying (online harassment), affecting 1 in 5 or 6, roughly 20 percent, and
5. Meeting an online stranger, the least common risk, around 9 percent (1 in 11), rising to 1 in 5 in Poland, Sweden and the Czech Republic.

In several countries, 15-20 percent of online teens report a degree of distress or feeling uncomfortable or threatened online, which suggests (arguably) the proportion of teens for whom risk poses a degree of harm.

Additional studies, conducted by US researchers Sameer Hinduja and Justin Patchin, corroborate Livingstone's numbers for cyberbullying and correlate suicide with bullying incidents:

- 15-35 percent of students are victims of cyberbullying,
- 10-20 percent of students admit to cyberbullying others
- Youth who are bullied, or who bully others, are at an elevated risk for suicidal thoughts, attempts, and completed suicides.
- Cyberbullying victims are 1.9 times more likely to have attempted suicide (offenders are 1.5 times more likely) than those who were not victims or offenders.[7]

Rochester Institute of Technology Study: Majority of cyber-offenses involving children and teens are perpetrated by their peers. [8]

In 2008, the Rochester Institute of Technology released a study on Internet behavior, which was the result of an eight-month evaluation of 40,000 students in fourteen school districts in Monroe County, New York. The regional study revealed, among other things, that:

- Most children begin using the Internet at Kindergarten age or younger.

---

[5] Livingstone, Sonia, "EU Kids Online," (cf. page 20, http://www.lse.ac.uk/collections/EUKidsOnline/Reports/EUKidsOnlineFinalReport.pdf)
[6] Livingstone, Sonia, "EU Kids Online," (cf. page 20, http://www.lse.ac.uk/collections/EUKidsOnline/Reports/EUKidsOnlineFinalReport.pdf)

[8] Report of the Rochester Institute of Technology, "Survey of Internet and At-risk Behaviors," by Samuel C. McQuade III, Ph.D. and Neel Sampat, RIT Center for Multidisciplinary Studies, June 18, 2008 ("RIT Study").

- The more time youth spend online, the more likely they are to engage in or experience cyber issues, such as cyber-abuse.

- The majority of cyber offenses involving children or teens are perpetrated by peers of approximately the same age and/or grade level.

- Cyber bullying and victimization begins as early as second grade and peaks in middle school.

- In high school, cyber offenses include piracy, bullying and data snooping.

The RIT study provides a good assessment for the types of issues and threats kids are facing. While the study is regional in nature and is not a national study like the Kaiser Family Foundation report, it is significant for a few reasons. First, it reveals that children are encountering cyber-issues in elementary school, which demonstrates the need for media literacy and digital citizenship education at the primary school level. Educators and parents should not wait until middle school to address Internet safety issues with chidren. Second, the study confirms that the "old paradigm of adults preying on children has been replaced with the new reality that kids now regularly prey on each other online."[9] Findings such as these put all stakeholders in a better position to prepare for and address these issues.

Further studies reveal other risks:

Sexting[10]

- 20 percent of teens (13-19) have electronically sent or posted online, nude or semi-nude pictures/video of themselves (22 percent girls; 18 percent boys)
- 33 percent of young adults (20-26 years) "are sending or posting nude or semi-nude images of themselves" (36 percent female; 31 percent male)

Reputation[11]

- 70 percent of recruiters and HR professionals in the U.S. said they have rejected candidates based on information they found online; while only 7 percent of consumers thought their online information affects the job search.
- 75 percent of companies in the United States require their hiring personnel to do online searches of job candidates.
- Reputation matters. Among U.S. recruiters and HR professionals surveyed, 85 percent say that positive online reputation influences their hiring decisions at least to some extent

III. RECOMMENDATIONS FOR HOW TO SUPPORT SCHOOLS

The JSCC Terms of Reference requests recommendations for "ways to support schools to change their culture to reduce the incidence and harmful effects of cyber-bullying." In response to this request, we submit the iKeepSafe Digital Citizenship C3 Matrix along with recommendations on how all stakeholders can become involved in the prevention and intervention of cyber-abuse and other online risks.

iKeepSafe Ditigal Citizenship C3 Matrix™

[9] RIT Study at p. 6.
[10] The National Campaign to Prevent Teen and Unplanned Pregnancy , "Sex and Tech: Results from a Survey of Teens and Young Adults," 2008: http://www.thenationalcampaign.org/sextech/PDF/SexTech_Summary.pdf
[11] Microsoft/Cross-Tab Study, "Online Reputation in a Connected World," 2010. http://www.microsoft.com/privacy/dpd/research.aspx

iKeepSafe partnered with noted security and education expert Davina Pruitt-Mentle along with other thought-leaders to produce the iKeepSafe Digital Citizenship C3 Matrix,[12] a guide to help educators and curriculum writers identify essential areas of study and levels of proficiency, based on age. The C3 Matrix outlines three levels of competency for students (basic, intermediate, and proficient) within the comprehensive C3 topics: cyber-safety, cyber-security, and cyber-ethics. Ideally, students will achieve proficiency in all C3 topics before matriculation.

New research shows that most teachers do not feel equipped to address questions from students on C3 issues. A new study, released in the US, February 2010, by Dr. Pruitt-Mentle and the National Cyber Security Alliance (NCSA), looks at C3 educational policies, initiatives, curriculum, and practices currently taking place in the US, K–12 schools.[13] Among key findings in the study, only five percent (5%) of teachers indicated that they had had a discussion with students about "how to make decisions about sharing personal information on the Internet"—the most likely Internet threat youth face online. Only 50 percent of teachers felt prepared to discuss cyberbullying; and only 15 percent of educators have actually had classroom discussion about it.

Other important C3 concepts that rarely came up in classroom discussions include: electronic plagiarism, sexting, the authenticity of information online, Facebook/MySpace use, downloading music and video files or identity theft—all essential elements of digital citizenship. A few C3 topics that returned a statistical zero for classroom conversations included: "managing your online reputation, cyber stalking/creeping, and using strong passwords"—again, these are critical skills that youth must have to successfully navigate the online world.

While 69 percent of teachers feel that C3 professional development is a priority, 44 percent of teachers have not taught any topics related to cyberethics, safety, or security in their classroom for the last year. More than half of administrators and technology coordinators agree that their school or school district requires that C3 curriculum be taught in the classroom, but over 75 percent of teachers have spent less than six hours on any type of C3 professional development education within the last 12 months.

Bystander Awareness and Professional Development

iKeepSafe recognizes that educators are in a unique position to encourage a culture of active bystander awareness. As a digital culture, we have not yet begun to mine the emotional and psychological data that kids offer up to peers online. As Web content becomes increasingly user-generated, kids are revealing more online about their state of mind, leaving telltale indicators or "bread crumbs" of their well being. In this setting, other users (bystanders, professionals and peers) are in a position to reach out to at-risk youth—those showing an interest in self-destructive behaviors such as suicide, eating disorders, self-mutilation, or drug and alcohol abuse.

On another level, bystanders are in a position to improve the general Web environment and behavior of all users by self-enforcing acceptable behavior for citizenship. All Web users, particularly teens, benefit when bad behavior is reported. Experiencing real consequences for online behavior helps

[12] iKeepSafe Digital Citizenship C3 Matrix (attached), available for download at http://knowwheretheygo.org/c3matrix.
[13] The National Cyber Security Alliance 2010 Study can be found at: http://www.staysafeonline.org/content/ncsa's-national-k-12-studies

teens understand that online communications are public, and though they may feel anonymous, all digital interactions can be traced by service providers and law enforcement back to the user.

Professional development and media literacy training will help educators identify at-risk youth, train them how to respond, and provide a network of support that can reach out to all aspects of online risks. Digital literacy, with an emphasis on professional development, is an essential subject that should be incorporated into the curricula of all schools. With curriculum already packed, digital citizenship requirements may create a new burden for educators, but the education community plays a vital, pioneering role in digital citizenship. Schools need to offer more flexible, in-depth professional development in cyber-safety, security, and ethics for all teachers, not just the technology coordinator or media-literacy specialist.

To make this training most effective, we encourage the JSCC to engage the public-health community for information and ideas on how to identify and reach at-risk youth in their online as well as real-world activities. A bold, new partnership, forged between public health, education, and government will help all parties recognize the indicators of risk and offer intervention, prevention, and bystander awareness to at-risk youth. For medical and education professionals trying to reach at-risk youth, online social media is a data mine. Intervention through electronic means, by online peers and professionals, has proven extremely effective in some instances.

Investment in professional development for teachers across all disciplines will see the greatest return in their students' ability to protect themselves and the infrastructure (in the case of security), while benefitting the positive resources available online. Educators are compulsive teachers: if they have the information, they will share it—even if it doesn't fall under their specialization. This is the future of digital citizenship education and training. The best way to train ethical, responsible, and resilient cybercitizens is to have ethical, responsible, and resilient teachers who are comfortable navigating the digital world.

Building a Network of Support

iKeepSafe has identified seven stakeholder groups that can influence outcomes during a cyber-incident. Stakeholders need to know how to protect students, themselves, and the school from abuse, thereby increasing positive outcomes for students and staff while minimizing the risk of legal complications. Stakeholder groups are:

1. Parents
2. Educators (i.e., teachers, technology teachers, counselors, librarians, and Safe & Drug-Free Schools)
3. School administrators
4. Public health and medical professionals (including school nurse)
5. Law enforcement (i.e., School Resource Officer, District Attorney, Sheriff)
6. Network Administrators (i.e., CTO and CIO).
7. Policy leaders to build the infrastructure—laws required for investigation and prosecution of child abuse, sexual enticement of a minor, harassment, etc.

A thorough network of support will promote education, prevention, bystander awareness, intervention, and reporting where possible. Network of Support tools should ensure that cyber

events receive appropriate documentation for legal purposes and reach out to the victim, perpetrator, and bystanders of an incident. Working together as a cohesive group, stakeholders can lay the groundwork that will prepare everyone involved.

- **Pre-incident:** Prepare for an incident by (1) developing policy, (2) implementing prevention/intervention programs, and (3) establishing specific protocol for incident management.
- **At the time of incident:** Identify strategies for how best to respond to the *victim, perpetrator, and bystanders* of an incident (i.e., fact finding, documentation, and reporting when necessary),
- **Post-incident:** Follow-up with the parties involved to determine appropriate actions and track outcomes at two, four, twelve, twenty-four weeks, etc. Review policies should be in place to assist schools in determining if they need to expand or revise their prevention strategies, and intervention efforts to reflect emerging trends.

Technology Solutions

iKeepSafe would like to see governments worldwide provide incentives for companies that volunteer to operate under acknowledged best practices and innovate safety measures. As new online risks emerge, so do new technologies. No one-size-fits-all solution will address the myriad of online risks; we must, therefore, employ a multi-layered approach to combating risks.

The YouTube Safety Center is an example of a multi-layered approach involving technology and rules. YouTube's new Safety Mode is a technology solution developed in response to an Internet risk involving youths' exposure to adult material on YouTube. Safety Mode gives YouTube users the option to choose not to see mature content that they may find offensive. When you opt in to Safety Mode, videos with mature content or that have been age restricted will not show up in video search, related videos, playlists, shows and movies. Comments default to collapse, and when opened manually, inappropriate words are hidden. Because Google knows that not all filters are 100 percent accurate, it provides users with other layers of safety, which contribute extra protection. For example, Google relies on the use of community flagging whereby a user can flag videos that may not be appropriate for YouTube. Moreover, objectionable comments posted by users on videos can be hidden. Safety Mode on YouTube does not remove content from the site but rather keeps it off the page for users who opt in.

iKeepSafe would like to see similar features deployed in the virtual world community. Today, virtual world sites, like WoogiWorld, are designed specifically for younger children and offer a range of safety settings that can be set by the parent. In addition, these sites offer training in digital citizenship. However, many virtual world sites and games involve the mingling of children and adults, which can present risks as children come into contact with violent or adult content. Ideally, children might participate in the communities and games on these sites and still be sheltered from violence and adult content. For example, if these virtual worlds sites enabled users to rate each other so that if a particular user is aggressive or engages in more violent activity, another user would know that and choose not to engage with that user. Also, players showing high levels of good citizenship could be rewarded within the virtual world with extra points or virtual money. eBay developed a good model whereby the community rates sellers and

buyers so that a new user is able to determine whether he/she would like to interact with that user. Something similar should be developed in the virtual worlds community.

Likewise, there is a critical need for virtual world sites and user-generated content sites to provide clearly marked information on how people can report abuse on the site. YouTube has developed a system whereby videos can be flagged and reviewed. Many Internet Service Providers provide one click access for reporting abuse. However, not all websites offer clearly marked procedures, which is something that sites should be encouraged to provide.

CLOSING REMARKS

iKeepSafe commends the JSCC and larger internet safety community in Australia for its proactive approach to protecting youth online and preparing them to be full digital citizens. We hope to be helpful as we work towards our shared priority of protecting children online.