Point Smart Click Safe!

<http://www.pointsmartreport.org/>

In June 2008 a diverse group of representatives from technology companies, child advocacy and parents' groups, educators, health researchers and policymakers gathered in Washington, DC to begin work on a set of recommendations for best practices that participants in the Internet industry could adopt to help keep children safe and smart when online. The result of the year-long effort is the report *PointSmart.ClickSafe.: Task Force Recommendations for Best Practices for Online Safety and Literacy*.

During the course of its work, the task force recognized, explored and considered a number of insights relating to child online safety including: the existence of an “ecosystem” of shared responsibility for child safety; the challenges to managing online risks, and the limitations of current technology and public policy for implementing online safety features. The task force also recognized the many existing and useful best practices that are already being employed by many companies in the Internet industry, as well as the work being done by a variety of other groups seeking to provide enhancements to online safety, such as the Internet Safety Technical Task Force convened by the Berkman Center for Internet & Society at Harvard University, and the extensive work that has already taken place in the United Kingdom by Dr. Tanya Byron and by the U.K. Home Office. The *PointSmart.ClickSafe.* Task Force worked to harmonize all these existing elements as it worked to develop its best practice recommendations.

In order to maximize harmonization, the *PointSmart.ClickSafe.* recommendations for best practices are designed to span all sectors of the Internet industry and are intended to be applied selectively based on a company's role and the types of services it offers that a child might use or with which he or she might come into contact. Embracing a child-centered perspective, the *PointSmart.ClickSafe.* best practice recommendations address three separate, but overlapping, categories of children's online experience - before they go online, during a child's online activities, and when problems arise - and recommend best practices for each of these stages. In addition, the task force recommendations recognize that a singular focus on safety is insufficient and that children need to learn digital and media literacy skills to help them think more critically about their activities and the online content they consume and, increasingly, create.

While the centerpiece of the task force's work has been to develop the recommendations for best practices that companies within the Internet industry can implement, it also recognizes that while the issue of online safety - like the Internet itself - spans many audiences, stakeholder groups, and jurisdictions, most Internet safety efforts have been both fragmented and granulized to the local level where there is often a significant lack of coordination and resources. More coordination at the national level supplemented with adequate resource development is needed. To this end, the task force recommends that policymakers consider the following steps:

* 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.
* Designation by the President or Congress of a *lead* federal agency that would work collaboratively and comprehensively with all major stakeholders in marshaling resources for the improvement of online safety and Internet literacy and coordinate the activities under diverse federal programs.
* 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 the nation’s diverse children and families about how to manage media.
* 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.
* Support digital literacy and online safety efforts by providing funding for: **Research** on the learning potential of digital media; **New modes of assessment** and evidentiary standards; **Professional development** for teachers; **Curriculum development** and implementation for students; **Public awareness campaigns** for parents and families; and **Research designed to identify, highlight, and promote best practices** and further solutions to improve digital literacy and fortify online safety.

Finally, recognizing the pivotal role of industry in ensuring steady improvement in this field, the task force suggests that voluntary activity strongly supported by industry is likely to be significantly more effective than legislated or mandated solutions; and that “light touch” regulation in this area is the superior approach for encouraging resource-rich companies to design progressive and innovative solutions, both now and in the future.

Children worldwide are presented with unprecedented opportunities and challenges in today's digital environment. All stakeholders - parents, teachers, child advocates, health professionals, providers of Internet access and content, law enforcement officials, and other concerned citizens - have a shared responsibility to ensure that a child's use of digital technology, and particularly the Internet, is as safe and enriching an experience as we can make it.

∗ ∗ ∗

The Internet, and in particular the “World Wide Web,” began life as a novel - and by today's standards - static venue for researchers. It has since morphed into a massively interactive and dynamic “cyber domain” for all comers that has added a new dimension to our social structure. The world is now connected as never before, featuring the ability to learn, create, engage and participate 24/7 on a global scale and in a way that has transformed communications, personal relationships, and business transactions.

Yet with the Internet, a marvel of our age, come many age-old problems. The same social issues -bullying and other inappropriate behaviors - that exist on the playground or in the mall also take place, and in some instances can be magnified, on the Web. Most adults, who have grown into the use of Internet-based communication tools, products and services as they were created, understand these issues, and the potential pitfalls and even dangers that can exist with them. But today's children encounter these issues in digital space without the adult mediation and instruction that occurs more frequently in offline situations. And some children who are more at risk offline, are also at greater risk online. Therefore, it is essential that there be multiple mechanisms to help them gain an awareness of the pitfalls and their consequences, as well as the behavior and social skills to avoid them.

Our task as adults is to understand our responsibility for helping children reap the full benefits of the Internet, while at the same time ensuring their safety. This task is challenging in the cyber world, where changes occur by the hour, borders and boundaries are sometimes warped, and parents and kids can operate in different universes, with different expectations and assumptions about technology. Reaching common understandings therefore can be difficult. But just as adults share responsibility in the physical world for helping children make the best of opportunities while ensuring their safety, they need to understand the shared responsibility in the digital world. As Dr. Tanya Byron has written:

*I believe that alongside new technology we need a new culture of responsibility, where all in society focus not on defending our entrenched positions, but on working together to help children keep themselves safe, to help parents to keep their children safe and to help each* *other support children and parents in this task.1*

In short, there exists an “ecosystem” of shared responsibility where each aspect of the network and its users are represented, and the perspective of each stakeholder involved with ensuring that children use the Internet in rewarding and safe ways is taken into account.

**A Child's Digital World**

Today's children are digital citizens from day one. In the digital world, we document their birth on video, and share photos by mobile phone, email, Web sites, and social networks. Our digital kids watch DVDs, listen to CDs and play digital learning games as toddlers. We keep grandparents and other family members in touch digitally with emails, videos, and photos. In elementary school they become participating cyber citizens, part of the 250 million North Americans regularly online.2 Parents check on them via mobile devices, they research school projects online, and submit homework to teachers' Web sites. They connect with each other using text messaging - which has to a large extent replaced voice and email contact among youth - and within their new community, by social networking sites, which are used weekly by 71% of youth ages 9 - 17.3 Their entertainment includes creating and uploading content and downloading and remixing that of others, or entering imaginary worlds to play games of logic or skill, all the while listening to an iPod or other MP3 device, watching TV and carrying on multiple online conversations. All told, kids and teens spend more than 6.5 hours per day in front of media screens.4

What specifically are children doing online? Youth participation differs depending on age, ability, and the availability of technology. The research staff of the Center on Media and Child Health (CMCH), Children's Hospital, Harvard compiled the following examples.

**Internet use and online environment by age group:**

**Young kids (ages 3-6)** This age group is learning to use the computer and is often on the Internet with parents, siblings, or teachers. Children are familiar with digital screens from television, but now are able to explore new interests that are challenging, exciting, and creative as opposed to the passive relationship with a TV show. They can:

* Watch video-sharing sites with their parents to explore interests and access things that appeal to them but are inaccessible in their own communities,
* Follow their TV interests onto the Internet through the connection between TV shows and associated Internet sites, reinforcing their relationship to characters, and
* Utilize educational games and activities that are divided into categories that focus on many of the skills designed to prepare preschoolers and Kindergarteners for formal schooling.

**Middle kids (ages 6-10)** This age group is facile with a computer and the Internet. Children are online every day for school assignments and recreation, including:

* Advergaming (e.g. branded games),
* Pure recreational gaming and free flash games,
* Moderated chat situations in walled garden sites,
* Expanding interests with new information rather than simply exploring established topics, and
* Homework.

**Tweens (ages 11-13)** To all of the above, new and more portable technologies are added for these youngsters:

* Cell phones and texting,
* Chat situations, which are not always moderated,
* Heavy video/computer gaming, and
* MP3 devices such as iPods and music downloads.

**Teens (ages 14-18)** All available digital and connected technologies are in use by teens:

* Social networking sites,
* Viewing, creating, and posting content on user-generated content sites,
* Downloads of music, videos, and TV shows,
* Writing code (e.g. widget, programs, and blogs), and
* Mash-up sites.

At the same time that adults help youth develop the technical skills to participate in this society, children must also be taught how to build the necessary habits and ethics to interact with respect towards others. Appropriate digital citizenship includes topics such as etiquette, communication and literacy, security, health and wellness, and rights and responsibilities.

It is also critically important to understand that a child's online actions produce a trail of digital footprints -- public information that can enhance or degrade their reputation and influence the course of their lives. For example, college admission administrators and potential employers scan the Internet to review applicants based, in part, on the sum of their postings online. For an instructive diagram of the responsibilities that face youth in the digital world, see

**Perspectives of Stakeholders in the Ecosystem**

As discussed in the preface, in June 2008 the *PointSmart.ClickSafe.* Summit was convened in Washington, DC by iKeepSafe, Common Sense Media, Cable in the Classroom (the cable industry's education foundation) and NCTA. Focusing exclusively on child online safety, a variety of participants drawn from stakeholder groups - including leading child safety advocates, parents groups, Internet service providers, online content providers, software companies, educators, law enforcement officials, and federal policymakers - shared their perspectives and discussed “best practices” for online safety, marking the first time such a broad cross section of online safety stakeholders came together for such a discussion. The *PointSmart.ClickSafe.* Summit was organized around four “panels” of stakeholders: 1) parents and parenting groups; 2) members of the education community; 3) representatives from the public health and safety community; and 4) representatives from companies providing online content and/or Internet access. The following outlines the perspectives offered during these panels. For a full summary of the panels, their key findings and recommendations

**Parents and Parenting Support Groups Panel**

This panel restated the basic principle that parents are, and should always be, the primary protectors of their children. Parents and caregivers teach their children how to take care of themselves, most likely using the same examples and processes that their own parents used. That works when parents are familiar with the issue (e.g., crossing the street safely), but it is evident that many parents are insecure about the use of Internet technologies. The panel showed that parents:

* Need to be empowered with tools to become familiar with the digital world,
* Lack awareness of the convergence and mobility of technology,
* Are less clear about their parenting role related to technology, and
* Do not have equal skills and/or commitment to children's education and safety.

In addition, a 2008 iKeepSafe survey, *The Parent Project,5* in collaboration with CMCH at Harvard Medical School, was one of the first studies about parents and the Internet and offers key insights. It revealed that parents have strong feelings and real fears about what their children encounter online, and what education they would like leaders to provide for safety and security:

* 89% - How to protect kids from online predators
* 81% - What parental controls are available and how to use them
* 79% - Information about how predators lure children
* 77% - How to implement Internet safety practices at home
* 71% - Kids and chat/social networking sites
* 70% - Links to Internet safety resources in each state
* 69% - Kids and instant messaging

**Education Panel** Education, by its nature, can play a positive role. Schools already teach students to use technology as a tool for learning. In addition to technical skills training, schools are in a position to provide safety information and the ethics perspective that children need. The panel had these observations:

Teaching:

* Improvement is needed in Internet safety education in schools, including professional development for educators and dedicated space in the curriculum.
* Appropriate online behavior and expectations should be taught across society to students, parents, and adults.

Policy:

* Education is governed at the state level but implemented at the local level, resulting in a disjointed effort, and
* Decisions are made far away from the classroom and often become a barrier to teaching.

Technology:

* Schools are often required to use filtering, but it is an imperfect tool and schools sometimes over-rely on it to the detriment of teaching youth about safety and responsible online behavior, and
* Filters are limiting because they sometimes block harmless and legitimate content and also fail to address quality and/or accuracy of information and skills.

Involvement and Access:

* Educators need cross-sector involvement with all stakeholders, and
* There are access equity concerns (e.g., Is Web 2.0 available to students both at home and at school?).

**Public Health and Safety Panel**

Health professionals see first hand the need for children to acquire those skills that lead them to become positive contributing members of society. They recognize the impact of technology and its influence on youth in the following ways:

* Youth have a sense of community within technology that adults lack,
* How youth use and interact through digital products affects how they feel about themselves, and
* Health professionals want youth to become responsible, ethical, and resilient cyber-citizens.

**Internet Industry Panel**

A number of best practices for online safety are currently employed by many individual companies and organizations in the Internet sector, either as a part of their overall corporate responsibility efforts or as a part of brand protection and extension, and many of these were put in place primarily in response to strong consumer demand. Indeed, the panel noted that there are continual innovations to online safety practices as companies compete to provide the best tools and resources for parents and families. The panel also noted that practices tend to include multiple components, such as the provision of parental controls or other tools, information about the use of the controls, information about media literacy, and partnerships with expert third party and/or non-profit advocacy groups.

A number of challenges for developing tools and information for parents and other consumers were noted. These include the proliferation and rapidly changing nature of platforms; the fact that the Internet “knows no borders;” and that no one “silver bullet” solution seems to exist. There was also the acknowledgement of the tension between wanting to provide truly empowering tools to parents while at the same time avoiding censorship or undue restrictions.

**(Footnotes)**

* 1. Byron, T., Safer Children in a Digital World, 2008.  
     2. Internet World Stats, www.internetworldstats.com, 2008.  
     3. Gruenwald Associates, Creating & Connecting - Research and Guidelines on Online Social and Educational Networking, Web Wise Kids, 2007.  
     4. Roberts, D. Foehr, U., Rideout, V., Generation M: Media in the Lives of 8-18 Year-olds, Kaiser Family Foundation Study, 2005.  
     5. The Parent Project, iKeepSafe, funded by the Department of Justice, Office of Juvenile Justice and Delinquency Prevention, Award Number 2006-MC-CX-K016, 2008.

When discussing online safety for children, it is important to recognize two key components of the topic: the technology upon which many online safety tools are based, and the public policies in place designed to ensure public good and well being. Both of these components offer advantages for online safety and both present limitations to ensuring that children are perfectly safe.

**Technology**

The task force reviewed and discussed four technology models designed to help protect children online: filters, monitoring software, information agents and alerts, and age verification. Multiple vendors provide a variety of these products. Some work well, others less so.

**Model 1: Filters** A filter is both loved and hated. When it prevents a child from coming across inappropriate content, it is great. When it is incompatible with a business transaction it is not only counterproductive but also costly. Parents, while praising a filter's effectiveness to stop a child's inadvertent access to pornography, can also be confused and frustrated by instructions and settings that differ from product to product. Educators admit that young people can often get around filters and fear that public reaction to just one negative incident could be enough to end use of technology at school. And if that negative incident did occur, the legal ramifications are unclear because case law for school situations related to the Internet is not well established.

Content that should be filtered out must first be indexed into a corresponding database. If it is not indexed in, it cannot be filtered out. In the end a filter can only be as good as its design and data. By definition, it will never eliminate 100% of the inappropriate content.

The following is a sample of the limitations connected with the purchase, installation, and use of filters:

|  |  |
| --- | --- |
| **Need** | **Current Situation** |
| Parents want to purchase a filter | No standardization or benchmark exists to differentiate an excellent from a merely good or mediocre product. |
| Filter installation in the home | Youth often install computer and Internet tools for untrained or uninformed parents and when doing so bypass the protective settings. |
| Default settings in the home | When set incorrectly the default can result in a total G-rated experience, limiting adult access to more mature and perhaps enriching content. |
| Default settings in schools | Overly restrictive settings chosen by some school systems often lock out harmless and valid educational materials. |

**MODEL 2: Monitoring Software** Monitoring software serves as a complement to or as a substitute for filtering. This software will track chat, email, web sites visited, downloads, etc., and in some versions allows parents or monitoring personnel to follow children's activities in real time, and to take control of those activities. Its strength is that through transparent access it provides an atmosphere of accountability; its weaknesses are the ease by which it can be hacked and the time it takes to review all of a child's online activities on a routine basis. For older children, monitoring software may have an impact on the trust relationship between parents and children.

**MODEL 3: Information Agents and Alerts** Information agents and alerts, such as Google Alerts, RSS feeds, etc., are tools that allow users to search and gather content based on personal specifications. The alert searches defined terms and provides users with a link to the specified content that has been posted on the Web, allowing the user to seek its removal. In the Web 2.0 environment, agents could potentially be programmed by parents to follow a child's movements and actions. If the child attempted to post or upload information defined by the parent as inappropriate, such as a personal phone number, the agent could intervene to ask, “Do you really want to do that?” The agent becomes both a monitor and a conscience.

**MODEL 4: Age Verification** Age and identity verification technology attempts to prevent youth from accessing adult or problematic content or certain youth sites outside their own age group, and to keep adults and possible predators or bullies from violating children's safe spaces. Often, verification involves a user reporting their birth date, or entering credit card information. Other technologies currently in use to verify children's ages are expensive, unavailable for widespread use, and can be compromised in some of the following ways:

* Youth and adults lie about age and fabricate identity information to register on sites restricted by age.
* Kids often have access to parents' credit card information and can use that to circumvent some verification strategies.
* Technology developed to detect youth by slang expressions associated with specific age groups is ineffective.
* Sensitive personal data held by a site to validate a child's age could be subject to fraud.

On the adult side, the issues with age and identity verification become even more complex:

* Adults seeking to do harm lie about age and identity.
* Decisions must be made about whether to even allow any adults on youth sites.
* Some trusted adults might enhance the online experience for youth, but how are they to be identified when most crimes against children are committed by acquaintances perceived as trusted?

These examples are only a fraction of the issues surrounding age or identity verification. For a detailed report on this topic, please see the research, discussions, and recommendations in the Berkman Center's *Internet Safety Technical Task Force*.

**Policy, Legislation, and Individual Rights**

When challenged to establish a safe environment, often the first inclination is to ask that regulations be established. In the U.S. 32% of the homes have children.1 How are children to be protected in those homes while the other 68% of homes are allowed and encouraged to access and utilize legal content? The following tenets must be accepted when reviewing policy, legislation, and rights:

* Tragedy, fear, and media coverage, rather than facts, often drive policy.
* The online safety issue is nonpartisan.
* There is substantial public concern that safety tools are not as effective as they could be.

Where technology allows for new freedoms and creative abilities it also produces situations that test the Constitution, the ethics of business, and the patience of parents. How many parents know that their 16-year-old has a constitutional right to safe sex information? How many teens know that it can be illegal to send (via the Internet or mobile phone) a semi-naked picture of themselves to their boyfriend or girlfriend (a relatively new phenomena known as “sexting”)? The scope of issues that deal with rights, law, and policy is vast. Some of the issues include:

* On the Internet, content harmful to minors is the hardest to regulate.
* Many Web sites with dangerous or disturbing content exist in other countries and are beyond the scope of U.S. regulation.
* Many social networking sites are places where minors and adults can interact.
* At-risk youth pose a different and greater set of challenges.
* Some Web sites drive traffic to themselves through deceptive means, such as intentionally using misleading meta tags and descriptors.

Privacy laws regulate the type of information that may be collected and how that information may be used. To address growing concerns from privacy advocates, policy makers, and government regulators, a number of steps have been taken.

The task force looked at gaps or limitations in policy and practice that impact the online safety of children. One major challenge in that regard is many real world laws do not necessarily exist or apply to the digital one.

**Examples of discrepancies**

|  |  |
| --- | --- |
| **Regulated or illegal** | **Unregulated** |
| Child pornography imagery | Violent speech |
| Online obscenity (based on community) | Foreign Web sites |

What should adults be required to do to protect under-age users? The following are a few examples of what issues must be addressed in order to keep minors safe:

* Access and screening:
  + Adult chat rooms accessed by credit card transactions must continue to offer a high confidence level that the entry is limited to adults.
  + Providers should continue to have the prerogative to screen and manage content according to company and publicly-announced guidelines.
* Privacy:
  + How does one protect young people who make themselves vulnerable when they share passwords and move in and out of each other's e-mail accounts and Web sites?
* Other issues to address:
  + How can industry fulfill government requirements for managing user online activity without assuming the role of police?
  + Legislation enacted in the fall of 2008 empowers the Federal Trade Commission (FTC), Federal Communications Commission (FCC), National Telecommunications and Information Administration (NTIA), and Department of Education (ED) to study children's online safety. Can four agencies moving independently yield first-rate, coordinated, efficient, cost-effective, and timely results? And what role can and should industry play in these efforts?

Technology is constantly changing but our overarching core values must remain constant. Rather than becoming fixated on a one-size-fits-all legislative response to the problem of the day, attention must be focused on those core values. Best Practices lead us in this direction. They provide the most direct potential benefits, because they empower the private and nonprofit sectors to create solutions and allow government to focus on broad policy guidelines rather than detailed, prescriptive, onerous or problematic laws and regulation.

**(Footnotes)**

1. [US Census Bureau, 2008 Statistical Abstract of the United States](http://www.census.gov/compendia/statab/tables/09s0058.pdf).

The PointSmart.ClickSafe. Task Force was convened to develop a set of best operating practices for companies in the Internet industry. To determine which practices are needed in this dynamic digital environment, the task force participants adopted a child-centered perspective. The results of this ecosystem-wide review and discussion of the landscape addressed three separate, but overlapping, categories of children's online experience:

1. Before children go online,
2. During the online activities of children, and
3. When problems arise.

Before one can determine what constitutes best practices, however, the nature of the Internet must be considered. First and foremost, it must be understood that the central role of the Internet is to enable access to information and freedom of expression. Second, it must be understood that the Internet is a dynamic and interactive environment. Users are generating, uploading, and sharing content with both individuals and communities. And third, the Internet industry is very diverse ranging from large global providers to small locally run services.

As stated by a 2009 report on improving the state of online safety and Internet literacy from The Berkman Center for Internet & Society at Harvard University

*A technology or combination of technologies designed for one environment or for use by one type of service provider may not be able to provide the same level of effectiveness in a different context. Each site has its own unique architecture, equipment, and operations, so integration of new software requires careful planning and testing in order to avoid unintended consequences or even site outages. Thus, any technological approach must be appropriately tailored for the context in which it operates, given the wide range of services on the Internet.”*

*Furthermore, “Some technologies may offer improved safety, but may have harmful public policy consequences and unintended consequences for youth and parents that outweigh the safety improvement. A balanced perspective is particularly critical in light of the Internet's central role in enabling freedom of expression and access to information from around the world. (Berkman, p.27)*

As acknowledged by Berkman and stated here in other sections, the quest for improvements in online safety is occurring among an interconnected web of interests that are focused on various Internet behaviors, threats, and activities. Therefore, as Berkman states, “A combination of technologies, in concert with parental oversight, education, social services, law enforcement, and sound policies by social network sites and service providers” is needed to help children mitigate the risks and actuate the benefits of the Internet.

**What Constitutes A “Best Practice”?**

It should be easy for parents and others to find clear and simple explanations of what information and safety elements exist, how they function, and what a user can do in various circumstances. Therefore, best operating practices should:

* Use clear and common language,
* Be consistent and transparent, and
* Provide information and tools that can vary by age and stage of the user.

These best operating practices should be crafted so that they can be:

* Modified for a specific service or application (e.g. ISP, blog, chat, social network),
* Scaled based on the number of intended or actual users,
* Designed and created as part of the product development cycle, and
* Continuously updated to reflect growth and change in the application or service.

**Best Practice Recommendations for  
Companies in the Internet Industry**

Ensuring children's online safety is a difficult and complex task that calls for input from and action by a wide variety of stakeholders. There is no “silver bullet”—no single technology or approach that has proved effective. Rather, what is required is:

* A combination of different technologies,
* Continuing digital literacy education for parents, educators, and children, and
* Active participation by all concerned companies, groups and individuals.

Similarly, a singular focus on safety is insufficient. Children must learn to minimize risks but also learn appropriate and ethical behaviors in this digital world. In addition, they need an understanding of media literacy, in order to be able to think critically about the content they consume and increasingly create. Therefore, best practices must be part of a larger effort to provide an entertaining, educational, and safe experience for children.

**Before Children Go Online**

**1. Education and information**

Basic information and education about the digital landscape must be in place and available to all children, parents, educators, and caregivers so they can understand the various risks, what constitutes appropriate behavior in different online spaces, and what options they have in services and terms of use. In addition, children need to learn how to use the technology efficiently, effectively and ethically so that they can participate fully in social, economic and civic life in the digital age. Best Practices should also encourage and empower parents, educators, and caregivers to understand the technology so they can make informed initial and ongoing choices for their children's safety and security.

**We recommend the following:**

1.1 Provide access to information that will educate parents, educators, and children about media literacy and ethical digital citizenship, and help them think critically about the content consumed and created on the Internet.

1.2 Make safety information for users, parents, and caregivers prominent, easily accessible, and clear.

1.3 Provide information that is easy to find and access from the home page, available during registration, and that can also be found in other appropriate places within the Web site or service.

1.4 Include specific information or FAQs about the services offered by the provider, especially safety tools and how to use them (e.g., conducting a safe search, setting filtering options, defining and setting appropriate privacy levels).

1.5 Provide links to additional resources that offer relevant safety and security information.

1.6 To make messages about online safety clear and easily recognizable to a variety of users, consider using consistent themes, and common words and phrases. Provide messages in multiple languages as appropriate.

**2. Registration/creation of user profiles**

**We recommend the following:**

2.1 Provide a clear explanation of how information collected at registration and set up will be used, what is public vs. private on the site, and a user's ability to modify, hide, and prevent access to user information.

2.2 Make safety information available during the registration process, prominent from the homepage and in appropriate places within the service (e.g. welcome email/message, point of sale information).

2.3 Provide information in the terms and conditions and elsewhere that defines acceptable behavior, states that users are not anonymous and can be traced, and details the consequences of violating the standards of behavior.

2.4 Provide notice that violating terms or conditions will result in specific consequences, including legal ones if required.

**3. Identity authentication and age verification**

The task force acknowledges that the issues of identity authentication and age verification remain substantial challenges for the Internet community due to a variety of concerns including privacy, effectiveness, accuracy, and the need for better technology in these areas. The Berkman report, for instance, concluded that:

*Age verification and identity authentication technologies are appealing in concept but challenged in terms of effectiveness. Any system that relies on remote verification of information has potential for inaccuracies. For example, on the user side, it is never certain that the person attempting to verify an identity is using their own actual identity or someone else's. Any system that relies on public records has a better likelihood of accurately verifying an adult than a minor due to extant records. Any system that focuses on third-party in-person verification would require significant political backing and social acceptance. Additionally, any central repository of this type of personal information would raise significant privacy concerns and security issues.*

**Therefore we recommend the following:**

3.1 Continue to explore age-verification and identity-authentication technologies and work to develop better safety and security solutions and technologies, keeping in mind that not all online environments may benefit from identity verification.

**During A Child's Online Activities**

Best Practices in this area should recommend how technologies can be used to define and control a child's digital activities and help parents establish the technology structure that they determine best meets their family values and needs as children grow and become more self-sufficient.

**We recommend the following:**

**4. Content screening**

4.1 Initially set defaults at a moderate level as a minimum, but instruct users in how to customize settings for their own needs.

4.2 Information should be provided about company policy on filtering, including the default settings, explanations of the meanings of different safety, security and filtering options (e.g., what is blocked by certain levels of filtering), how to make adjustments, and when settings might need to be reapplied (e.g., a new version).

4.3 Consider carefully the placement and highlighting of sites belonging to and designed by children and youth (e.g., a child's profile page could become a “safe zone,” don't locate children's content near ads for adult-targeted materials).

4.4 Consider a “walled garden” approach when relevant with products aimed at children eight years of age and younger.

**5. Safe searching**

5.1 Include specific information about how to conduct a safe search, how to set filtering options, and an explanation of privacy settings.

**When Problems Arise**

To provide the best response to problems, we recommend:

6.1 Have in place a robust procedure, backed by appropriate systems and resources, to handle complaints. Ideally, each company should have an Internet-safety staff position or cross-functional team charged with supervising the procedures and resources and given the authority and resources to be effective.

6.2 Provide a reporting mechanism visible from all relevant pages or sections of a site or service.

6.3 Consider providing a designated page with relevant information and instructions about how to submit a report or complaint including:

* How users can determine the appropriate individual or agency to contact when reporting a problem (e.g., customer service, law enforcement, or safety hotline) and links to these services.
* What types of content and behaviors should be reported, the reporting procedure, and what supporting information might need to be included.
* How to remove unwanted content or information from a user's page or profile.
* How to cancel an account.

6.4 Cooperate with law enforcement, where applicable, and follow all relevant statutes.