November 9, 2005

The development of ***Kids Online in Schools: Risk Management and the Law***, by Dr. Parry Aftab © 2005 was funded, in part, by *Kan-safe*, a project of the South Central Kansas Library System, South Hutchinson, KS.

Utilizing funds from a 2005 LSTA (Library Services and Technology Act) Grant award from the Institute of Museum and Library Services, Kan-safe was able to contract with Dr. Aftab to provide enhanced Internet safety content to be made available on Kan-safe at http://kan-safe.info.

The online guide outlines legal issues in terms of privacy, access, security and authority as well as various other Internet related issues that parents, students, librarians and educators face.

We trust that you find Dr. Aftab's guide to be an invaluable resource.

Larry Papenfuss
Kan-safe Project Director

Kids Online in Schools: Risk Management and the Law

By Dr. Parry Aftab

According to recent surveys, almost all public schools have Internet access. (Some have Internet access in only their libraries or technology or media centers.) Yet most parents I talk to and most who have responded to our surveys tell us they have no idea how their children's schools are using the Internet or what their children do online at school.

The schools need to recognize that parents are an important part of the team. And if parents don't know what their children's schools are doing, they should be asking these questions and offering their support and help. Encourage them to do that and let them know the kinds of questions they should be asking. It's the only way we can make sure that our children are getting the most out of the Internet, safely.

That said, parents may be the biggest part of the problem. Even when a school delivers programs on Internet safety and responsible use for parents, few attend. They mark-up the acceptable use policies or refuse to sign them. Yet, they are the first to complain about not having the tools and information they need to keep their children safe online.

While this guide will be discussing some important laws and how they impact safety and risk management in the school. You will notice it is less about the wording or exact coverage of the laws themselves and far more about the legal approach. The laws will change, but most often the legal approaches don't. Instead of memorizing what exists today and worry about what will be adopted tomorrow, think in terms of privacy, access, security and authority. All laws relate to one of these four important issues. If you learn to spot when they are impacted or implicated, you'll be fine.

Before we go further, though, probably the best advice I can give schools is to provide parents with as much information as they can, as often as they can. One of the first things a lawyer learns is that clients are less likely to be unhappy if communication is good. Even if they are unhappy with the content of the communications, a well-informed client is a happier one. It stands to reason that a well-informed parent is a happier one too. And less likely to come charging into the administration offices or calling their lawyers.

Note that few schools have found the magic bullet. All are grappling with safety concerns, lack of adequate funding and technology training, and changing technology. They are also grappling with busy parents and some parental indifference. There doesn't appear to be any universal standard, with each school district handling the issue of Internet safety in its own way. (Sometimes school by school within the same district.)

Many schools have adopted policies and rules that the parents and students have to sign, before the students are permitted to use the Internet at school. Some are using filtering products. Others are sending notices to parents and setting policies for safe and acceptable use. Some are trying to regulate a student's activities after hours and off-premises. And many schools are finding themselves named in lawsuits for infringing on a student's free speech or other rights. And far too often, lose these lawsuits.

There is no “one size fits all” here. Solutions need to be customized to take into consideration the school’s technology uses and staffing, curriculum, students’ needs and behavior, parents’ concerns, and community values. And it is more a matter of awareness about the problem areas than the specific laws, that change often and vary jurisdiction by jurisdiction. All good lawyers know how to spot a potential legal problem. Good school administrators and educators, unfortunately, in these difficult times do too.

There are also new issues, such as cyberbullying and how far a school’s authority can extend, and social-networking websites such as myspace.com, xanga.com and facebook.com (among others) to grapple with and parental responses to deal with.

Where do we start? We all need to remember that we are still learning, often the hard way. Children are very innovative in abusing the Internet and each other. Just when we think we understand the risks and have worked out solutions, they surprise us with their innovations. But if parents, school administrators and school boards, teachers, school safety officers, students and librarians and library-media specialists work together, and keep the lines of communication open, we’ll keep making progress. All we have to do is hold out until this new generation of Internet-savvy students become parents, teachers and school administrators themselves. ☺

The Big 4 – Privacy, Access, Security and Authority

Privacy is perhaps the most legally risky area for schools. Several laws cover privacy. They cover the privacy of a student’s school records, their physical health and abilities, and even their disciplinary history. The two biggest laws impacting students’ privacy, perhaps, are FERPA (The Family Educational Rights and Privacy Act of 1974, often also called the “Buckley Amendment”) and COPPA (The Children’s Online Privacy Protection Act). (Both of these are discussed in detail in the Appendixes.)

I advise clients to always think in terms of “Kids, Cash and Kidneys,” when privacy laws are considered. It works as well for schools. Many issues involving children have special privacy protections. So do financial information (“cash”) and health information (“kidneys”). If kids, financial information or health information is involved, tread carefully. You are likely to step on one law or another. Does the student have special needs? While you may be able to spot anything that directly exposes that information, what about information about their using a special bus, or having special testing procedures? Indirectly, that can provide as much information about a child’s physically limitations as directly information someone that they are blind, deaf or in a wheelchair.

A good example regarding how privacy impacts the law, (when school surveys are involved) is set forth below:

The Protection of Pupil Rights Amendment (“PPRA”) was enacted in 1994. It requires that school districts obtain written parental consent before students can provide certain personal information for a "survey, analysis or evaluation." Although it only applies if the “survey, analysis or evaluation” is funded by a Department of Education administered program and students required to participate. In 2002 the PPRA was amended by the No Child Left Behind Act (“NCLBA”). The amendment (20USC 1232 h(b) requires parental consent for any required student participation in a survey, analysis or evaluation that would reveal information about:

- The students or their parents’ political affiliations or beliefs.
- The student’s or their family’s emotional problems.
- The student’s sexual behavior or attitudes.

- The student's illegal, antisocial, self-incriminating or demeaning behavior.
- Criticisms of members of the student's family.
- Legally-recognized privileged or fiduciary, such as those of lawyers, physicians or clergy.
- The student's or their family's religious beliefs, practices or affiliations.
- Family income (expect as otherwise required by law to determine eligibility for financial assistance).

The NCLBA also requires that school districts (together with parents) adopt covering the students' privacy rights and parents' rights to inspect instructional materials, administration of psychical examinations, compilation and collection of survey data and disclosure of students' information for marketing purposes. Parents are now also permitted to opt-out of certain non-essential surveys and physical examinations under 20 USC 1232 h(c). Even if you don't understand the law, or even know it exists, you can spot the hot issues, such as information about a student's family, beliefs and emotional issues.

Spotting Internet Problem Issues for Schools

While the Internet is a terrific educational tool, its use in schools does pose some problems. In addition to the issues parents face with children who access the Internet from home, there are a few issues that are specific to schools. These include what personal information the school may post on its website about the students, use of children's intellectual property and the intellectual property of third parties, and how to judge the difference between a bogus resource and a credible one. They also include hacking, plagiarism, and whether the school can discipline students for what they do on a personal website designed and posted from home. Cyberbullying and ID theft are on the rise, too. School administrators are dealing with angry teachers who are bashed online by students after hours and off-premises and threats of law suits every week. MySpace.com and similar social networking sites allow millions of people to search their sites for students from a particular school. And, last but not least, a chain e-mail that circulates among the students can crash a school's entire system and create terror in the hearts of an entire class of 4th graders.

Photos of students- to post or not to post…that is the question.

All of us are excited to send Grandma and Grandpa the photo of our child winning the local sports trophy or getting the debate award. Dog-eared clippings from our town paper are cherished and carefully glued into scrapbooks to show our grandchildren. So what's the harm in posting the same photo at the school website?

First of all, a website isn't a local newspaper. It's available to more than 700 million people worldwide. And the people who might use this information to reach your children aren't neighbors who are worried about what their neighbors think. They are strangers to your family and your community. (Polly Klaas, a young girl in the United States, was targeted from a mailing list compiled for marketing to teenagers in a particular zip code area. Her killer bought this list of girls between certain ages and chose her at random from the list. The list contained her address, name, and age.)

Although, to my knowledge, law enforcement in the United States has not yet encountered a case of a child molester targeting a child they found at a school website, they worry (and so do I) that someone will use this information to target a child. Just think for a moment. Children who appear on a school's website are at that school from 8:30 A.M. to 3 P.M. every day. It's easy to find them during those hours and when they are walking to and from school, especially if you know their name and have a printout of their photo in your hand. “Jennifer, can I talk to you a minute?” How many of our children wouldn’t respond to someone who knew their name?

So I recommend that a school use photos of children only after they get the parents’ consent, and only in groups of five or more. I also recommend that they not identify the children by name, only by the group: “Ms. Smith’s fourth grade class” or the “Volleyball Club,” for instance. This makes perfect sense when you think about it. We’d never let anyone post our child’s photo on a highway billboard, would we? We need to think of the Internet as a giant billboard posted on the largest superhighway in the world. If we wouldn’t allow something about our children to appear there, we shouldn’t allow it to be posted online.

In addition to being unsafe, it is also covered by FERPA (The Family Educational Rights and Privacy Act of 1974, often also called the “Buckley Amendment”), along with other personally identifiable information about a student. (Read the attached guide on FERPA for more information about what it is and what it covers at Appendix 1.)

Plagiarism

Kids have always been creative when it comes to avoiding schoolwork. They spend hours avoiding twenty minutes' worth of work. While most of us were limited to finding a smarter older sibling or friend to help us with schoolwork (or better yet, do it for us), our cyberkids can now surf the hundreds of sites that sell term papers to teens online. And they don't even have to retype them; they can just download them, typed and illustrated—ready to go.

Many of the smarter teachers I know have bookmarked these sites so they can routinely compare the student's submitted term papers with those they find online. There are also some very good commercial services that provide a plagiarism review service to schools. Also, since most of these term paper plagiarism sites provide the term papers only for a fee, advise parents to check out their credit card statements and make sure they are not subsidizing their children's plagiarism.

Off-School Websites

Just as kids have circulated derogatory jokes and drawings of teachers or their school mates over the generations, these digital kids circulate their jokes, insults, and drawings using the power of the Web, where they can be viewed by everyone. They then share the URL (Web address) of the site, so fellow classmates can appreciate their work. Often the URL ends up in the hands of a teacher. Teachers and administrators or parents of students who are the target of the site report it, and threaten to file a lawsuit or to report it to the police. The school then feels compelled to do something. Typically the child is suspended or expelled, or college recommendations are withdrawn.

Their reaction is understandable. But may be costly. The school may not have the legal authority to take action if the website or post is created off-premises, after hours and at the student's home. And civil rights advocacy groups and legally-savvy parents are quick to sue, and often win. When a school disciplines a student for creating a website, posting a message online or sending a digital communication (text-messaging, instant message, e-mail, etc.) outside of school grounds and school hours, it is treading on very dangerous ground.

The websites and messages vary from school bashing, administration and teacher bashing and student bashing, to cyberbullying and harassment of fellow students, vulgarities and threats, to encouraging others to hurt or kill others. Sometimes the students are just behaving badly, or are rude and hurtful, and sometimes they are committing serious crimes, including hacking, identity theft, vandalism and targeting victims for attacks by hate groups and predators.

Cases have challenged the school's authority in many states and federal jurisdictions under constitutional and procedural grounds. And the decisions conflict. There is some guidance from the U.S. Supreme Court on free speech issues in schools, but the last definitive case was decided during the Vietnam War. Most others issues will be resolved by lower courts and the law will vary depending on the state or federal district or circuit in which the school is located. So, before taking action it is essential that the school district seeks advice from knowledgeable counsel in this field. The normal school district lawyer may not have the requisite level of expertise to advise on this, and a constitutional or cyber-free speech lawyer may have to be retained.

There are a few generalizations we can provide, which can give some general guidance. But these cases are very fact specific and the facts in your case may differ from those in the cases already determined in your jurisdiction.

- Clear threats: If there is a clear-cut threat (one that is seen by both the person making the threat and those who have seen it or received it), the school is generally entitled to take action, including suspension and expulsion.

- Clearly disruptive of school discipline: If the school had proof that the speech has or will disrupt school discipline, the school has a better chance of succeeding. Ungrounded fear or speculation is not sufficient to support the school's burden.

- In-school activities: If the student is bringing in print-outs of the website, or promoting other students in school to visit the site, or if the student accesses the website while at school or creates or works on the website from school, there is a greater likelihood that the actions will not be deemed out-of-school activities and would fall within the school's authority.

- School-sponsored activities: If the website belongs to the school or is created as a school-sponsored project, it will fall under existing U.S. Supreme Court decisions permitting school authority.

- Cyberbullying: If a student targets another student using interactive technologies or the Internet, there is almost always an in-school activity related to the cyberbullying. Privacy-invading e-mails and harassing messages are often printed out and distributed in school and on school grounds. In addition, cyberbullying typically creates a disruption in school, where the victim is afraid, may seek counseling or miss school, their grades may be impacted and friends may get involved. Any proof of an in-school student impact will help support a finding of school authority.

- Cyber-staff harassment: If the school can demonstrate that the student's website or harassment has had a real impact on the staff, the school has a greater likelihood of success in upholding its authority. If the teacher or staff member quits in reaction to the harassment or take a leave of absence or seeks medical treatment to help deal with the emotional implications of the student's actions, the courts tend to be more sympathetic and are more likely to give the school the authority to discipline the student. Without this, the courts tend to lean towards leaving the staff member to other legal recourse.

- Social-Networking or Profile pages: Parents are panicking about their children posting blogs, online diary profiles and social-networking profiles at sites like MySpace.com, Facebook.com and Xanga.com. (I'll discuss more about this below.) These sites often list their members by school name and location. Schools are now beginning to take discliplinary action against their students for posting a page at one of these sites. Unfortunately, most of these posts are made from the student's home computer and after-hours. In all likelihood, the school will be sued and lose if they attempt to take disciplinary action against a student just for having one of these pages (assuming they are not harassing another student from the school from their profile page). The overall safety of a student in real life, and fear of their communicating with sexual predators is probably not sufficient grounds for a school to reach out beyond its traditional authority.

Schools are also attacked (often successfully) when they fail to follow their own procedures. Often pressured by angry staff members, other parents and fear of the problem growing out-of-control, they fail to adhere to their own written rules. They fail to give the requisite notice, in the requisite manner and allow the requisite respond period to lapse before calling a hearing. They sometimes fail to notify the parents and give the student's family a chance to respond. This is not a time for shortcuts or acting without careful planning.

Sometime the schools over-reach in their policy, attempting to prohibit speech too broadly. These policies are generally knocked down unless the school can demonstrate a practice that limits an over-broad reach and clarifies what is prohibited and what isn't for the purposes of the policy and school rules. One school even reserved the right to examine any home computer of their students, to determine whether a cybercrime or abuse has taken place using that computer.

The schools have a valid concern and legal obligation to maintain discipline and protect their students while in their care. But in this tricky area, especially when damages for infringing on the students' rights can exceed the annual salary of much needed teachers and other educational resources, schools cannot afford to guess. Until the law becomes better settled, the schools need to be careful before acting, seek knowledgeable legal counsel, plan ahead and get parents involved early.

So what's a school to do? Talk, educate and mediate…it's what schools do best. Bring in the students and parents. Create peers counseling and mediation boards. Set policy. Create awareness programs. They shouldn't panic or react in a knee-jerk manner. I would suggest they take their lead from a very experienced school superintendent.

A teenager in that high school, after getting angry with certain teachers and administrators, lashed out by posting some pretty vulgar and insulting things about them on a personal website. He wrote the site from home and posted it online. It wasn't posted on the school's server, but was available to everyone with Internet access once they had the URL. URLs of classmates' sites get passed around quickly, and many of the kids in the school accessed the site from the school's computers.

When the word got back to the teachers and administrators, they were understandably furious. They sought help from the police, who threatened to charge the teenager with harassment (but they wouldn't have been able to make that charge stick).

Everyone involved seemed to lose their head, but the superintendent managed to keep his. He recognized that this wasn't a school matter, and that the parents needed to be involved. He called in the parents, who were appalled and took this situation as seriously as they should have. Together they worked out a suitable apology and a way to handle the case without blowing it out of proportion. The press had a field day. This superintendent stood firm against the anger of the teachers and the pressures of the community. He was right.

Months later he shared something with me. He told me that he had met the young teenager at a school event, and the student apologized once again. He also thanked the superintendent for handling the situation with grace. The boy had acted out in anger, and hadn't thought about the consequences of his anger. Eventually, even the teachers came around. I was sorry my children were already out of high school—they would have benefited from attending a school system run by such a patient and wise administrator. We could use many more like him.

This advice works just as well when cyberbullying or social-networking use is discovered.

Death Threats/Bomb Threats

Innovative kids have been making school bomb threats for years, especially when the weather is good or they haven't studied enough for a scheduled exam. (When I was young, we used to have someone pull the fire alarm.) But, since the U.S. Columbine/Littleton tragedy, bomb threats in schools have increased dramatically and spread online.

Many schools now have well-developed safe-school teams who handle offline risks, like offline bomb threats, weapons brought to school, gangs, violent students, and protests. Some schools also use online filtering programs that are managed off-premises on third-party proxy servers. These programs provide monthly reports to a school about what sites its students have tried to access from their blocked lists. Typically, their blocked lists include bomb-building sites. Yet none of the schools I talked with review this information and share it with the safe-school team.

It would be easy enough for these reports to be shared, then compared with offline information on file with the safe-school teams. Schools need to know who is trying repeatedly to access bomb-building sites, so they can use this information to help handle the offline risks. It's information they already have—but aren't using.

These reports can be used for other safety purposes as well. One of the biggest problems schools face is not knowing when students are making threats or cyberbullying each other online. Students' websites are typically not picked up by the search engines, and finding a site that isn't listed on a search engine, unless you know its domain name, is like finding a needle in the virtual Internet haystack.

When a student builds a controversial or provocative website, usually the only ones who know about it are other students, who use the school computers to access the site. These reports can tell you when there is a sudden popularity of a certain site at a school. They should be regularly reviewed. It's the only way of spotting a student's website early. It's also one of the few ways a school's administration can use information to prevent violence in schools, because it can identify students who are crying out for help in advance.

Pen Pal Programs

One of the best ways of pairing students with other students around the world is through pen pal programs. School-to-school programs are the safest way of allowing students to communicate with strangers online. We need more of these programs, and we can only hope your child's school will help create them. Unless schools are part of a school-to-school pen pal program, parents should be informed about the pen pal program in the acceptable-use policy, and given the choice of having their children participate. There are many risks relating to non-school pen pal programs, so check out the services very carefully. Also, make sure that they give you what you need to comply with FERPA. And, if you need to provide personal information about students to register or allow the students to send their own messages, you should also be aware of COPPA (The Children's Privacy Protection Act) and the implications of providing consent without parents' approval. (See Appendix for a full analysis of COPPA.)

Cyberbullying and Schools

What is cyberbullying?: Cyberbullying is any cyber-communication or publication posted or sent by a minor online, by instant messenger, e-mail, website, diary site, online profile, interactive game, handheld device, cell phone or other interactive device that is intended to frighten, embarrass, harass or otherwise target another minor. If there aren't minors on both sides of the communication, it is considered cyberharassment, not cyberbullying. Most kids don't consider a one-time rude or insulting communication to be cyberbullying. They think it needs to be repeated, or a threat of bodily harm, or a public posting designed to hurt, embarrass or otherwise target a child.

What ages does it usually affect?: Cyberbullying typically starts at about 9 years of age and usually ends around 14. After 14 it usually becomes sexual harassment. Many cases of cyberbullying occur right after a child receives their first IM account when they often try to see what they can get away with. (These kids usually stop when they understand the consequences of their actions.)

How prevalent is it?: Very. 90% of the middle school students we polled admitted to having had their feelings hurt online. 65% of the students we polled between 8 and 14 have been involved directly or indirectly in a cyberbullying incident as either the cyberbullying, the victim or a close friend of one or the other. 50% have heard of or seen a website bashing another student in their school, and 75% have visited a bashing website. 40% have either had their password stolen and changed by a bully (locking them out of their own account) or had communications sent to others posing as them. Many studies that ask kids if they have been "cyberbullied" fall short of measuring the real problem. Only 15% of parents polled even knew what cyberbullying was.

How does it work?: There are two kinds of cyberbullying, direct attacks (messages sent to your kids directly) and cyberbullying by proxy (using others to help cyberbully the victim, either with or without the accomplice's knowledge). These include bashing website, where kids are encouraged to vote for the ugliest, fattest, etc. victim. Because cyberbullying by proxy often gets adults involved in the harassment, it is much more dangerous.

Why do kids cyberbully each other?: Who knows why kids do anything? When it comes to cyberbullying, they are often motivated by anger, revenge or frustration. Sometimes they do it for entertainment or because they are bored and have too much time on their hands and too many tech toys available to them. Many do it for laughs or to get a reaction. Some do it by accident, and either send a message to the wrong recipient or didn't think before they did something. The Power-Hungry do it to torment others and for their ego. Revenge of the Nerd may start out defending themselves from traditional bullying only to find that they enjoy being the tough guy or gal. Mean Girls do it to help bolster or remind people of their own social standing. And some think they are righting wrongs and standing up for others.

What's the profile of a typical cyberbully?: There are four different kinds of cyberbullying. They are motive-driven, based on the motives for the cyberbullying. They may use the same methods as the other kinds of cyberbullies, but the reasons for their actions are very different. Solutions require that we understand the motives involved to address them effectively.

The four types of cyberbullies include:

- The Vengeful Angel
- The Power-Hungry or Revenge of the Nerds
- The "Mean Girls"
- The Inadvertent Cyberbully or "Because I Can"

"The Vengeful Angel": In this type of cyberbullying, the cyberbully doesn't see themselves as a bully at all. They see themselves as righting wrongs, or protecting themselves or others from the "bad guy" they are now victimizing. The "Vengeful Angel" cyberbully often gets involved trying to protect a friend who is being bullied or cyberbullied. They generally work alone, but may share their activities and motives with their close friends and others they perceive as being victimized by the person they are cyberbullying.

Vengeful Angels need to know that no one should try and take justice into their own hands. They need to understand that few things are clear enough to understand, and that fighting bullying with more bullying only makes things worse. They need to see themselves as bullies, not the do-gooder they think they are. It also helps to address the reasons they lashed out in the first place. If they sense injustices, maybe there really are injustices. Instead of just blaming the Vengeful Angel, solutions here also require that the situation be reviewed ot see what can be done to address the underlying problem. S there a place ot report bullying or cyberbullying? Can that be done anonymously? Is there a peer counseling group that handles these matters? What about parents and school administrators. Do they ignore bullying when it occurs, or do they take it seriously? The more methods we can give these kinds of cyberbullies ot use official channels to right wrongs, the less often they will try to take justice into their own hands.

The "Power-Hungry" and "Revenge of the Nerds": Just as their schoolyard counterparts, some cyberbullies want to exert their authority, show that they are powerful enough to make others do what they want and some want to control others with fear. Sometimes the kids want to hurt another kid. Sometimes they just don't like the other kid. These are no different than the offline tough schoolyard bullies, except for their method. Power-Hungry" cyberbullies usually don't need an audience. Sometimes they may involve a small audience of their friends or those within their circle at school, but are really seeking the reaction fo their victim, not bystanders. Sometimes the power they feel when only cyberbullying someone is not enough to feed their need to be seen as powerful and intimidating. They then brag about their actions. They want a reaction, and without one may escalate their activities to get one.

Interestingly enough, though, a special profile of the "Power-Hungry" cyberbully is often the victim of typical offline bullying. They may be female, or physically smaller, the ones picked on for not being popular enough, or cool enough. They may have greater technical skills. Some people call this the "Revenge of the Nerds" cyberbullying. It is their intention to frighten or embarrass their victims. And they are empowered by the anonymity of the Internet and digital communications and the fact that they never have to confront their victim. They may act tough online, but are not tough in real life. They are often not a bullying but "just playing one on TV."

This kind of cyberbullying usually takes place one-on-one and the cyberbully often keeps their activities secret from their friends. If they share their actions, they are doing it only with others they feel would be sympathetic. The rarely appreciate the seriousness of their actions, and often resort to cyberbullying-by-proxy. Because of this and their tech skills, can be the most dangerous of all cyberbullying.

Power-Hungry cyberbullies often go away and find another victim if they don't get the reaction they are seeking. So "Stop, Block and Tell!" works well here. The Revenge of the Nerds type fear exposure, understanding that they would be the target of ther larger tougher kids in the playground if exposed. These react best when they know that few things are ever anonymous online. We leave a trail of cyber-breadcrumbs behind us wherever we go in cyberspace. And, with the assistance of a law enforcement or legal subpoena, we can almost always find the cyber-abusers and cybercriminals in real life. Shining a bright light on their activities helps too. When they are exposed, letting the school community know about their exposure helps prevent copycat cyberbullying.

Helping them to realize the magnitude of their activities is also helpful. Often their activities arise to the criminal level. The more this type of cyberbully understands the legal consequences of their action, the more they think about their actions.

Ignoring them can also be very effective. But sometimes, instead of going away when ignored, they escalate their actions to get others involved, through a cyberbullying-by-proxy situation. Whenever a Power-Hungry cyberbully is suspected, it is crucial that law enforcement is notified and that the victim keeps a careful watch on themselves online, through "googling themselves." They can even set a Google Alert to notify them by e-mail if anything new is posted online with their personal contact information.

"Mean Girls": This type of cyberbullying often (but not always) involves girls. But the cyberbullies are always "mean." The tough guys in Karate Kids were "mean girls" bullies and so is Malfoy in Harry Potter, even though they are boys. Mean Girls cyberbullying occurs when the cyberbully is bored or looking for entertainment. It is largely ego-based and the most immature of all cyberbullying types. In a vast majority of "Mean Girls" bullying situations, the cyberbullies are female. They may be bullying other girls (most frequently) or boys (less frequently).

"Mean Girls" cyberbullying is usually done, or at least planned, in a group, either virtually or together in one room. This kind of cyberbullying is done for entertainment. It may occur from a school library or a slumber party, or from the familyroom of someone after school. This kind of cyberbullying requires an audience. The cyberbullies in a "mean girls" situation want others to know who they are and that they have the power to cyberbully others. This kind of cyberbullying grows when fed by group admiration, cliques or by the silence of others who stand by and let it happen. It quickly dies if they don't get the entertainment value they are seeking.

The most effective tool in handling a Mean Girls cyberbullying case is blocking controls. Block them, block all alternate screen names and force them to go elsewhere for their sick entertainment. In addition,teaching the bystanders not to support the cyberbullying antics by voting at the Mean Girl's constructed bashing pages is crucial. They are never able to cyberbully their victims without the proactive help of others. The best way to stop them in their tracks is if they are threatened with loss of their AIM accounts, they wise up fast!

The Inadvertant Cyberbully: Inadvertant cyberbullies usually don't think they are cyberbullies at all. They may be pretending to be tough online, or role playing, or they may be reacting to hateful or provocative messages they have received. Unlike the Revenge of the Nerds cyberbullies, they don't lash out intentionally. They just respond without thinking about the consequences of their actions.

They may feel hurt, or angry because of a communication sent to them, or something they have seen online. And they tend to respond in anger or frustration. They don't think before clicking "send."

Sometimes, while experimenting in role-playing online, they may send cyberbullying communications or target someone without understanding how serious this could be. They do it for the heck of it "Because I Can." They do it for the fun of it. They may also do it to one of their friends, joking around. But their friend may not recognize that it is another friend or make take it seriously. They tend to do this when alone, and are mostly surprised when someone accuses them of cyberabuse.

Education plays an important role in preventing Inadvertant Cyberbullying. Teaching them to respect others and to be sensitive to their needs is the most effective way of dealing with this kind of cyberbully. Teaching them to Take5! is an easy way to help them spot potentially bullying behavior before it's too late. Netiquette training is essential here.

What's the profile of a typical cyberbullying victim?: Anyone age 9 to 14. After that, the bullying becomes more dangerous and usually involves sexual harassment. We consider this cyberharassment, not cyberbullying, because of the nature of the attacks and the age of the actors.

What can you do to prevent it? Educating the kids about the consequences (losing their ISP or IM accounts) helps. Teaching them to respect others and to take a stand against bullying of all kinds helps too. (Read more about this in "what role can education play in this" below.)

How can you stop it once it starts?: Because their motives differ, the solutions and responses to each type of cyberbullying incident has to differ too. Unfortunately, there is no "one size fits all" when cyberbullying is concerned. Only two of the types of cyberbullies have something in common with the traditional schoolyard bully. Experts who understand schoolyard bullying often misunderstand cyberbullying, thinking it is just another method of bullying. But the motives and the nature of cybercommunications, as well as the demographic and profile of a cyberbully differ from their offline counterpart. (To learn more about the methods that work best with the four different kinds of cyberbullies, read about "the profile of a typical cyberbully," above.)

What is the school's role in this?: When schools try and get involved by disciplining the student for cyberbullying actions that took place off-campus and outside of school hours, they are often sued for exceeding their authority and violating the student's free speech right. They also, often lose. Schools can be very effective brokers in working with the parents to stop and remedy cyberbullying situations. They can also educate the students on cyberethics and the law. If schools are creative, they can sometimes avoid the claim that their actions exceeded their legal authority for off-campus cyberbullying actions. We recommend that a provision is added to the school's acceptable use policy reserving the right to discipline the student for actions taken off-campus if they are intended to have an effect on a student or they adversely affect the safety and well-being of student while in school. This makes it a contractual, not a constitutional, issue.

What's the parents' role in this?: Parents need to be the one trusted place kids can go when things go wrong online and offline. Yet they often are the one place kids avoid when things go wrong online. Why? Parents tend to overreact. Most children will avoid telling their parents about a cyberbullying incident fearing they will only make things worse. (Calling the other parents, the school, blaming the victim or taking away Internet privileges.)Unfortunately, they also sometimes underreact, and rarely get it "just right."(You can read more about this in "Not Too Hot, Not Too Cold! Goldilocks and the CyberParents")

Parents need to be supportive of your child during this time. They may be tempted to give the "stick and stones may break your bones, but words will never hurt you" lecture, but words and cyberattacks can wound a child easily and have a lasting effect. These attacks follow them into your otherwise safe home and wherever they go online. And when up to 700 million accomplices can be recruited to help target or humiliate your child, the risk of emotional pain is very real, and very serious. Don't brush it off.

Parents should also let the school know so the guidance counselor can keep an eye out for in-school bullying and for how your child is handling things. You may want to notify your pediatrician, family counselor or clergy for support if things progress. It is crucial that you are there to provide the necessary support and love. Make them feel secure. Children have committed suicide after having been cyberbullied, and in Japan one young girl killed another after a cyberbullying incident. Take it seriously.

Parents also need to understand that a child is just as likely to be a cyberbully as a victim of cyberbullying and often go back and forth between the two roles during one incident. They may not even realize that they are seen as a cyberbully. (You can learn more about this under the "Inadvertent Cyberbully" profile of a cyberbully.)

Your actions have to escalate as the threat and hurt to your child does. But there are two things you must consider before anything else. Is your child at risk of physical harm or assault? And how are they handling the attacks emotionally?

If there is any indication that personal contact information has been posted online, or any threats are made to your child, you must run…do not walk, to your local law enforcement agency (not the FBI). Take a print-out of all instances of cyberbullying to show them, but note that a print-out is not sufficient to prove a case of cyber-harassment or cyberbullying. You'll need electronic evidence and live data for that.

Using a monitoring product, like Spectorsoft, collects all electronic data necessary to report, investigate and prosecute your case (if necessary). While hopefully you will never need it, the evidence is automatically saved by the software in a form useable by law enforcement when you need it without you having to learn to log or copy header and IP information.

What's law enforcement supposed to do?: First, they need to be trained to tell the difference between annoying communications and dangerous ones. They also need to understand how to investigate a cybercrime and how to obtain information from an ISP.

We advise that anyone who threatens your child physically, who is posting details about your or your child's offline contact information or instigating a cyberbullying by proxy campaign should be reported to the police. (Although you should err on the side of caution and report anything that worries you.) Using a monitoring program, such as Spectorsoft, can facilitate the investigation and any eventual prosecution by collecting and preserving electronic evidence. Print-outs, while helpful in explaining the situation, are generally not admissible evidence.) If you feel like your child, you or someone you know is in danger, contact the police immediately and cut off contact with this person or user, staying offline if need be until you are otherwise instructed. Do not install any programs, or remove any programs or take other remedial action on your computer or communication device during this process. It may adversely affect the investigation and any eventual prosecution.

Law enforcement can assist parents by steering them to their cyberbully's ISP. Most ISPs prohibit cyberbullying and harassment using their services and will terminate the cyberbully's Internet account. Sometimes this can be more effective than threatening the cyberbully with jail.

What role does awareness and education play in this?: Education can help considerably in preventing and dealing with the consequences of cyberbullying. The first place to begin an education campaign is with the kids and teens themselves. We need to address ways they can become inadvertent cyberbullies, how to be accountable for their actions and not to stand by and allow bullying (in any form) to be acceptable. We need to teach them not to ignore the pain of others.

Teaching kids to "Take 5!" before responding to something they encounter online is a good place to start. Jokingly, we tell them to "Drop the Mouse! And step away from the computer! That way nobody will get hurt!!" We then encourage them to find ways to help them calm down. This may include doing yoga, or deep-breathing. It may include running, playing catch or shooting hoops. It may involve taking a bath, hugging a stuffed animal or talking on the phone with friends. Each child can find their own way of finding their center again. And if they do, they will often not become a cyberbully, even an inadvertent cyberbully.

There are several ways we can educate kids not to support cyberbullying:

- Teaching them that all actions have consequences;
- Teaching them that cyberbullying hurts;
- Teaching them that they are just being used and manipulated by the cyberbully;
- Teaching them that the cyberbully and their accomplices often become the target of cyberbullying themselves; and
- Teaching them to care about others and stand up for what's right.

And, in addition to not lending their efforts to continue the cyberbullying, if given an anonymous method of reporting cyberbullying websites, profiles and campaigns, kids can help put an end to cyberbullying entirely. School administration, community groups and even school policing staff can receive these anonymous tips and take action quickly when necessary to shut down the site, profile or stop the cyberbullying itself.

We need to teach our children that silence, when others are being hurt, is not acceptable. If they don't allow the cyberbullies to use them to embarrass or torment others, cyberbullying will quickly stop. It's a tall task, but a noble goal. And in the end, our children will be safer online and offline. We will have helped create a generation of good cybercitizens, controlling the technology instead of being controlled by it.

What's the law?: All but a small handful of states in the US have cyberharassment or cyberstalking laws. Sometimes the cyberbullying falls under these laws. But rarely will law enforcement investigate them as a crime or prosecutors prosecute them as a crime. A few notable cases (one in NJ and other recent ones in Louisianna and Virginia) have take this tact. But most have not. In addition, many cases of cyberbullying (like their adult cyber-harassment equivalent) are not criminal. They may come close to violating the law, but may not cross the line. Most of the time, the threat of closing their ISP or instant messaging account is enough to make things stop. But sometimes, either because the parents want to make an example of the cyberbully or because it isn't stopping, lawyers need to be brought in. It may also be the only way you can find out whom is behind the attacks.

Social-Networking Websites and Blog Profiles

MySpace.com is currently one of the most popular on-line social networking services, especially among today's teen and young adult "netizens." Reporting over 34 million users in November 2005 and growing at a rate of 175,000 new registered users daily, it has become the hottest site for people to share information and interact with each other. Other similar sites are very popular as well, such as Facebook.com and Xanga.com. And they all allow a student to post their school and be searched by schools. Students are posting their photos, personal information and contact details openly on their profiles, as well as accepting communications from strangers contacting them from their profile pages.

Schools are concerned, understandably. But here, too many schools are suffering from the same knee jerk responses as in cyberbullying and teacher bashing incidents. Here, unfortunately, unlike cyberbullying when the victim is a student, or attacks against personnel at the school, schools do not have the requisite authority to do anything but ban access to these sites from a school computer. Nor should they do more. This is a parent issue, not a school one. Schools should focus on educating their students on safer Internet use and communications, and refer the other issues to the parents. Schools can offer workshops and programs for parents, but should not try and act like the parent.

Understanding more about how these work

This surge in popularity of profile sites could be attributable to the lure of the extensive collection of communication options offered by social-networking sites, or it may just be a manifestation of the faddish nature of today's young people. In any event, the sheer number (and relative ages) of its usual users, demands that it be realistically considered as a prime target of harassers, cyberbullies, child predators, scam artists, and other unscrupulous individuals.

Regrettably, from the standpoint of Internet safety and risk management, these sites suffer from the same two basic shortcomings that plague most other major providers of free communications services.

1. There is a VERY lopsided ratio of registered members to "moderators" available to enforce the site's Terms of Service (TOS). MySpace has approximately a dozen people to monitor all user activities on the site. Accordingly, they rely on the members to inform them when site policies have been violated.

2. Even when a violation IS substantiated, in most instances, there is an inherent inability to effectively bar an abuser from a free site. Since the information provided in the membership application is NOT routinely verified, it is relatively easy to open a completely fictitious account under a new persona.

So, What is the Answer?

Given these above realities, it is incumbent upon EACH user, schools (and the parents of minor users) to know the proper procedures for reporting abuse AND how to effectively deal with unwanted contact, harassment, etc. Before we discuss these factors, let's take a look at some of the specific aspects associated with MySpace.com:

Safety Issues

1. As mentioned earlier, there is no verification of membership information. Because of this, and the huge popularity of the site, it is NOT uncommon for underage minors to obtain membership despite the site's minimum age restriction of 14 years old. Given the relative social inexperience and trusting nature of young users, it can be expected that many may become the primary targets of child predators and other bad actors.

2. The members of MySpace rely heavily on the use of detailed "profiles" to find and meet others with similar interests. Although the user has primary control over what information is ultimately displayed, most minors are only too eager to provide as much personal information as possible. Despite the fact that inclusion of telephone numbers, street addresses, and last names in a member's profile are forbidden under the site's TOS, age and city/state of residence information is AUTOMATICALLY populated into a member's profile, based on the birthday and zip code fields required for completion of the initial membership form.

3. The site also provides a module designed for members to "rate" each other (from cold to hot), based on their photos and other profile content. While on the surface this may appear to a harmless exercise, such "comparisons" can be strong catalysts for "flaming," cyberbullying and outright harassment, especially among teenage members.

4. Another risk is that information regarding a member's school is encouraged to be inputted for support of the site's "Classmate Finder" service. This database can be searched by SCHOOL NAME and STATE in order to identify all members that may attend a particular institution. From the standpoint of protecting a minor's personal information, this can be VERY risky.

Despite the issues noted above, the management of MySpace.com genuinely desire to provide a safe and enjoyable social venue. This is manifested in several recent undertakings:

1. Very comprehensive Terms of Service guidelines have been developed for the site. These appear to be more in-depth than then those published by similar sites and specific restrictions are clearly outlined (www.myspace.com/misc/terms.html).

2. When it is suspected that a member does NOT meet the minimum age restrictions, the site is very responsive regarding parental requests to terminate their membership. (They encourage the parent to do this with their child first, as a lesson in responsible and safe Internet use.) If they learn that someone is underage, they delete their profiles and terminate their membership, unilaterally.

3. The site administrators have enlisted the help of WiredSafety.org and me to provide a comprehensive on-line list of safety "tips" and to make recommendations for how the site can educate its users about safe and responsible Internet use. Such information is intended to better protect its members from harassment, exploitation, etc. It is strongly recommended that ALL current and prospective members review the pages which can be found at:
http://viewmorepics.myspace.com/misc/safetytips.html?z=1&Mytoken=20050605155359.

So How Can a School Help a Parent Protect their Child from Becoming a Victim?

Virtually **ALL** of the experts that are concern with Internet safety, as it pertains to minors, agree that the **MOST** effective way to accomplish this is by the **PARENT** becoming integrally involved in their child's on-line activities.

The actual depth of this involvement depends largely on the amount of trust that a parent has in knowing that their child understands what should and should **NOT** be done when "surfing" the 'net. The amount of trust shown will almost certainly vary with age, level of maturity, and past performance.

Some parents take the direct approach by restricting Internet access to times when they (the parents) are available to physically monitor the child's use. Others may resort to the installation of monitoring software so they can view a child's surfing habits, after the fact. (We like Spectorsoft's products, which you can find at spectorsoft.com or software4parents.com.)

Indirect methods rely on the fact that a set of Internet usage "rules" have been agreed upon by both parties and that the child will not only abide by this agreement, but will be completely forthcoming if they inadvertently experience "trouble" on the 'net.

Some parents may decide to take the middle ground by locating computers in central areas around the home, such as dens, living rooms, etc. Usually, they will configure the system to automatically block access to certain chats, pornographic sites, etc. The belief is that a child will be less likely to try to surf prohibited sites, or engage in other risky behavior, if their actions can be readily viewed by other family members.

Regardless of what actions a parent may choose to take, the reality is that kids will be kids and that, curiosity, peer pressure, or just plain boredom will sometimes trump common sense and caution. In other words, either by ignorance or design, a minor **CAN** be expected to get into trouble, at some point in time. When this happens, it will be up to the **PARENT** to step in and take the appropriate actions.

However, proper PREVENTION can help drastically minimize the odds of your child becoming a victim of exploitation, cyberbullying, and/or on-line harassment. Knowledge **IS** the key. Accordingly, it is suggested that parents and their children openly discuss what your children are doing online and the possible dangers related to Internet use. A very good start would be to JOINTLY browse the various pages at http://www.wiredsafety.org/safety/index.html. Here you can find comprehensive information and additional links pertaining to all facets of web safety. (Our Internet safety information at InternetSuperheroes.org uses the popular Marvel comic characters, such as Spider-Man and The Incredible Hulk, to teach children safe, private and responsible technology use.)

We need to make sure that parents remember that the greatest single risk our children face in connection with the Internet is being denied access, and that we have a solution for everything else. If you let your children know that you are there for them if things go wrong online or offline, you will have done the single most important thing to keeping them safe. You are the first line of defense when it comes to keeping your children safe. Be worthy.

What to Do If A Student Experiences Problems on MySpace

Both technical (site functionality) and non-technical difficulties (harassment, inappropriate behavior, etc) can be reported through a central "**Contact MySpace**" email system that can be accessed via a prominently displayed tab at the bottom of their primary navigation pages.

Upon selection, a form will be displayed requesting the following information:

- "Name" (or MySpace nick)
- "Email address"
- "Phone number" (if personal contact is desired of deemed necessary)
- "Subject" (pull-down list of common topics available, or OTHER)
- Description Box (be as detailed as possible)

This form is the primary contact method for almost ALL problems, requests, suggestions, and general comments. However, one MAJOR exception to this policy….that is in the area of account cancellations. The on-line form states "We will not honor delete requests sent via this form."

To learn how to delete an account at MySpace.com, check out the safety tips posted on MySpace.com by me under their front page "safety" tab. They are very responsive to school administration, if there is ever a problem. You can also contact me for help directly, at parry@wiredsafety.org.

Exactly What Information are the student Broadcasting to the World?

Publishing a public profile is a great way to meet others of the same age group or that may share similar interests. For members, it is a quick way to establish common ground for subsequent communications with others.

However, profiles can also provide unscrupulous individuals with preliminary information that can lead to a user being targeted as victim of malicious attacks or exploitation by scam artists and/or child predators. Even the inclusion of photographs can spur harassment. For example, any ethnicity that is obvious in a published photo can draw immediate racial slurs from bigoted members. A provocative or sexually suggestive picture will invariably result in contact from those with strictly prurient interests. A pic of an obvious minor is also sure to draw the attention of your typical cyberbully, or worse, a child predator. In essence, the question is "What constitutes too much information?" Generally, the following guidelines should ALWAYS be considered if using a public profile is desired:

- **Never publicly post in ANY online forum any personally identifiable information.** What is personally identifiable information? It's any personal information that could be used to find or identify you in real life. This could be such information as your real name, address, telephone number, cell number, your sports team, health club, or links to websites or other profiles that might give this information away.

- **Even without meaning to, you can give this information away** by taking a pic in front of your car with your license plate, home address, workplace, school, etc showing in the photo. You may be wearing a school or team t-shirt, a scout uniform or baseball cap that might give away ways of finding you offline. This information could be misused to steal your identity, guess your passwords, cyberstalk, cyberbully or harass you or by predators who really want to hurt you.

- **Always keep in mind that some individuals will maintain contact with the intent to glean as many small bits of information as possible.** When viewed as a whole, these seemingly innocuous facts can used to determine a prospective victim's actual location. They may use multiple screen names and user profiles, pretending to be other people, to gather more information from someone who might not be willing to continue talking to a stranger beyond a few conversations.

- An easy guide for kids, tweens and teens is to **tell them never to post anything that their parents, principal and a predator shouldn't see.**

- On a related note, **NEVER post any information or pictures that you would NOT want to be broadcast to the entire world.** Remember, once you hit that send button, you will have virtually NO control over how this information will be used, or who may end up viewing it. A typical scenario involves one member persuading another to send them sexually explicit pictures of themselves. This can eventually lead to threats of publishing the pictures Internet-wide, or forwarding them to a victim's friends, coworkers, and family members. Can you even imagine the level of embarrassment you may be forced to suffer?

It would be very prudent schools to search for their students, by school, frequently. On MySpace, as with most similar services, this can be done by simply (although you might have to register as a member to do so). Anything that you believe is inappropriate should be immediately brought to the student's and parent's attention. Students should be reminded of WHY such information is dangerous. Monitoring software, such as Spectorsoft.com, can also keep parents apprised of any changes in their child's pages. (To learn more about this, read the appendix section taken from my new book, Internet Safety 1-2-3!)

Teaching Our Children Critical Thinking and Media Literacy Skills

It costs thousands of dollars to publish a book. Cable and television programming costs even more. Magazines carefully check facts and universities use peer-review methods to make sure that what is published is accurate and credible. But anyone can publish a website, in a few hours, and say anything they want—often without a credible basis for it. So, how can anyone know when they have a real and credible site or just someone's puffery? It's not easy. Online there is no stamp of approval for quality control. A site published by an anti-Semitic group that claims the Holocaust never occurred may look as real and sound as reliable as a scholarly university dissertation. And when our children come across it, it might become the research source for their term paper on World War II. Schools are facing this issue frequently these days. So teaching children how to evaluate the credibility of a site is an important part of using the Internet in connection with schoolwork. Essentially, it's teaching them to be good information consumers.

Every year I hear about a school that has assigned a visit to MartinLutherKing.org for their students on Dr. King's birthday. Someone obviously has not done their homework. It has clear bias and is reputed to have been created by a racial supremist group. And this information is well known enough that a parent would be understandably concerned if they found the site assigned to their children. Even if the teachers aren't aware of the site's reputation, they should be using their own information evaluation methods before assigning any website to their students.

I am sure you have your own program for reviewing credible online information and websites. But have included some simple thoughts below, just in case. Whenever we find a website, we should think about the purpose of the site. Is it designed to sell something? If it's designed by anyone who sells anything, you have to assume that it's designed to at least indirectly promote its products or services. Any site that is designed to sell something should be approached as critically as any offline promotion or advertisement.

Once we understand the site's point of view, we can evaluate what they are saying more effectively. Our children already know, at a young age, the candy bars or hamburgers that are smaller than they appear on television, or the toys that are constructed poorly, or the computer game systems that need optional equipment at additional cost in order to do what is promised. One of the first legal rules our children learn is caveat emptor—buyer beware. Teaching them to use critical judgment when reviewing a website is easy. The information gathered from a website should be accurate and current. And if there is a bias, the website's bias should be obvious, and the authority of its writers should be set forth.

Here are a few things teachers and their students should be checking when they visit a site to conduct research:

- Who's the author or website creator, and what's their authority? Is it written by Nobel Peace Prize Award winners, or by Joe Crackpot? While many won't tell you that they are unqualified to make the statements they make at the site, they leave clues. Our children should look first to the credentials offered at the site for the site authors. If the person states that he is a professor at Outer Siberia University, you should check for links to the university. Has the person listed awards? If so, are there links to the entities that gave the awards so you can check? Is this person a published author? If so, does Amazon.com, Barnes & Noble, or Borders have his book listed online? Search for other sites that reference this person. Not every one is an award-winning professor and published author, but most good sources are cited elsewhere online.
- What's the bias of the site? Whose points of view aren't covered? Bias isn't necessarily bad, as long as it is clear to the site viewer. Remember that everyone has their bias, but some are more significant than others. Is this a site that performs "unbiased" reviews of advertisers? If so, have they disclosed that fact to the readers? Are they a nonprofit entity with a particular mission or purpose? Where was the site created? Is it from an international group that might have a country or culture bias? Is it a U.S. site which might have a U.S. bias? Often, you can detect bias by reading closely. The good sites will identify their mission. Think about who is creating the content, whose points of view are included, and whose are excluded. Students should try to achieve balance by including different biases and points of view when they do their research.
- How current is this information? Does the page have a "last updated" date notation? Many of the sites I researched for this book, including many on finding credible resources, were last updated in 1996. When I reviewed their content, I took that into consideration. Certain things don't change, such as how to judge credentials, but other things, like branded and approved site lists and what schools are doing, have changed radically. The site I looked to for current information was updated a few months earlier, and gave that date on the front page. If the site doesn't contain a "last updated" date, look to see if there's a "recent additions" or "what's new" section of the site, and see how often it is changed. You want to make sure the content is updated often, since it tells you two things: that the site gets regular attention, and that it contains recent information. A good site is updated regularly, preferably at least once monthly, and, with news and hot topical sites, more often than that. If you can't tell when a site was last updated, send an e-mail to the webmaster at "webmaster@[the name

of the site].” Ask how often the site is updated and the date it was last updated.

- Is the information stable and consistent? Is the information consistent within the site? Does everything match the theme of the site and this information? Are they proposing censorship on one page and free speech on another? (I’m not talking about CNN’s site, where they seek to present alternate and opposing views.) Is this the only site that espouses this viewpoint, or is there other support for this position? Have you compared it with related resources? Often, a site that appears too good to be true is too good to be true. Most good sites, with well-supported positions, will have support from other sites.
- What have they linked to? Do the links work? Do they link to credible sites, and do credible sites link to them? Are the links correctly described? Are they current? Who else links to them? Again, is the link information updated and accurate, or do the links not work anymore? The school and public librarians are the real experts in judging credibility of resources. That’s what they do when they select resource and reference books. Talk to them about how they are teaching your children to exercise informed information judgment. They are helping build your children’s information literacy skills.

Getting Parents Up to Speed and on Board

The best way for schools to get parents involved is to let them know what’s going on. Every survey I have done with parents tells us the same thing: No parents know what’s going on at their child’s school with the Internet, and many parents don’t know what the Internet is or how it works. Yet every school laments the fact that the parents aren’t more involved, and parents complain that they’re not included. (What we have here is a “failure to communicate.”)

So the simplest way to get parents involved is by letting them know what’s going on (I call that the “notice rule”), getting their consent to anything that has increased risks (I call this the “informed consent rule”), and educating them so they can be a part of the decision making and the solution.

Notice and Informed Consent

Schools need to tell parents how they are using the Internet at school, what the risks are, and how they are managing the risks. The notice has to be clear and complete, and lay out all the important information in a way even the most computer-illiterate parent can understand. And it should be included in the acceptable-use policy the school prepares and hands out to students and parents.

Whether they filter or not, every school should have an acceptable-use policy, which is a list of the rules pursuant to which children (and others) are permitted to use the Internet. Some school systems like to formalize the process, making it school board policy, with all the formalities that entails (notice, hearings, etc.). Others adopt it on a school-by-school basis as they do most rules, such as no running in the hall, and no smoking on school grounds. But however they do it, every school needs one.

Given all the controversies about safe schools and how schools use the Internet, I am amazed to find how many schools haven’t yet adopted acceptable-use policies. I recently spoke before a group of principals from one of the largest cities in the United States. I was shocked when they told me that they had been considering adopting acceptable-use policies for almost two years but hadn’t yet done it. That’s when schools face legal liability. Waiting two years to set rules about what kids can and can’t do online? Why? Once they understand the risks, schools should move quickly to set safety rules and get the parents informed. If the formal process is taking too long, create an informal one, and get the notice out to parents and students.

There's no magic to creating an acceptable-use policy. I've been doing them for years for major corporations, and schools are the same. And, although we cyberspace lawyers hope you will hire us to help us feed our children and pay their college tuitions, you don't even need a lawyer. But the policy does need to tell parents and kids how the Internet is being used and what the rules are, as clearly as possible, as well as what happens if anyone breaks the rules.

I have included a suggested provision to handle off-site and afterhours abuses, such as cyberbullying and teacher bashing. Before adopting anything, check with your school board attorney and see if it conflicts with your local policies and laws, or how it needs to be adapted for your needs.

Setting the Framework

Here's what should be determined in setting the policy and in disclosing it in an acceptable-use policy:

- How is the Internet used at school? Is it in the library only, library/media/tech center only? In the classroom?
- Who supervises Internet use?
- What are the special rules for use at each location?
- What are the risks? Chain e-mails? Chatting? E-mail? Instant messaging? Accessing inappropriate sites? Giving out personal information online? Posting nasty things about others? Copyright infringement? Piracy? Hype and misinformation? Threats of violence? Bomb threats? Doing things that cost money?
- Are filtering software or filtering services used? How do they work? What are the risks of overblocking (innocent sites being blocked) or underblocking (inappropriate sites getting through)? What can be done if a student needs to access a site that is blocked? Are there override mechanisms? Can the site lists be modified to allow a school to add an innocent site to the allowed lists or an inappropriate site to the blocked lists?
- What's the rule about downloading materials? Have the students been warned of the risks of viruses and the seriousness of hacking?
- Are school directories, with telephone numbers and student and parent names, posted on the school website? What about class rosters? School team members and the schedules for games, etc.?
- Can students be disciplined for posting defamatory or provocative information about other students, the school or school personnel on personal websites composed outside of school? (Schools can do this only if they relate to school safety or discipline, unless the students and parents agree otherwise in the policy.) What are the guidelines?
- Is the school posting personal information about the student on a website? Do they post student e-mail addresses? Do they post student photographs? Individually or in groups? Are the students identified in those photographs? How are they identified?
- Is the school partnering with third parties on online content and programs? If so, are these programs making personal information about students under the age of thirteen available to these third parties? If they are, parental consent (not just school consent) is required before the information is provided to third parties.
- What information is collected about students' Internet activities? To whom is it disclosed? Is it available to parents upon request?
- Is the school posting student works on a website? Is there a student chatboard or e-mail system?

Can students sign up for Web-based chat?

- What happens if the students break the rules? Will there be a warning? Suspension? Check the school disciplinary process on due process and procedural issues.
- Once the school knows what the entire system looks like, it should describe it to the students and to the parents. (Remember that the parents may not all understand what the school is talking about, so using familiar terms and not a lot of cyber and techie terms is most effective.) Tell the students what they are allowed to do and what they aren't. Let them know the consequences of disobeying the rules. Then explain the risks and get the parents' okay.

Explaining the School's Choices

If the school chooses not to filter, explain this in simple terms. Tell the parents and students why the school decided against filtering, and how it came up with a safety plan that it believes will be effective. If parents are informed, they can decide what risks are appropriate for their children and consent to those risks. If schools merely send home a consent form without the requisite disclosure, that consent form isn't worth the paper it's written on. All consents, to be effective, have to be fully informed consents. Besides, if a child ends up spending millions at an auction site, schools want the parents, not the school, to be responsible. That's another reason schools should want the acceptable-use policy signed by the parents.

And if the parents won't sign the form, the school should make sure the child doesn't have school Internet access. Otherwise, the school faces potential liability. Treat it the same way you would have a school field trip permission form. No form – no trip!

Let the Parents Decide

Parents, armed with sufficient accurate information, are the best ones to make decisions about their children's safety. Is there a dispute over when a child's photograph can be posted at the school's website? Let the parents decide. Tell them what the controversy is—some parents and students want the fame and attention, while others are worried that this could fuel a pedophile's attempts to contact the children. Lay out all the risks. And give the parents the choice.

If the school wants to make sure it is absolved of the risks and claims relating to those risks, a waiver alone isn't sufficient, since students themselves have claims that cannot be waived by the parents. An indemnification from the parent is the only way the school can make sure it is covered. However, when parents agree to indemnify and hold the school harmless from any such claims, the parents have to bear the risks of their child suing after reaching the age of majority—as long as the school fully disclosed the risks to the parents.

Getting them to agree on cyberbullying and school disciplinary procedures

While a school may not have constitutional authority to take action against a student who has build a bashing site offline or harassed another student from their home computer, they can easily obtain contractual authority through a creative use of their acceptable use policies. When parents and students sign the policies agreeing that the school can take action in a case where a student harasses a teacher, someone in administration or another student, the school can now act. It may be the best party to act to change this behavior, in any event.

You start here, just as you do elsewhere. You explain the problem. Then explain what you want them to consent to and why. Then you explain the consequences of violation of policy, once approved. See my suggestion, below:

“Recently we have become aware of certain activities by some students designed to target teachers, school administration and other students. These can take the form of threats, posting false or embarrassing information, identity theft, passing rumors or spreading false information, altering photos or posting sexually suggestive images of another student (real of manufactured), or setting them up for humiliation by creating a bashing site for others to vote for the most [fill in the blank] online.

We recognize that this has an immediate and direct effect on the well-being, morale and safety of our school community and students, and on the learning atmosphere in school. While these activities may be conducted off hours, from a home computer, interactive e gaming devices or the students’ cell phones and outside of a school sponsored or sanctioned event, we believe that we can and must take action to protect the school community, the students and personnel safety and well-being and to allow students to concentrate on their educational activities while in school.

By signing below, you and your children agree that we can impose disciplinary action against a student as though this activity had occurred within school, from one of our computers during regular school hours. [insert the disciplinary code reference.]”

Some schools have gone much further, reserving the right to search and seize a home computer that has been misused in a cyberbullying incident. I don’t advise that a school go that far, and frankly, have no idea why a parent might sign such a consent. (Perhaps it shows how few parents actually read what we want them to sign. ☺)

Build a Solid Team of Parents, Friends, Librarians, and Schools

As more and more schools and libraries are getting online, teachers and librarians are getting wired, too. (No, that doesn’t mean that they are doing anything they shouldn’t be doing ☺—it means that they’re getting online.) They’re a great resource for parents, teachers and school administrators. They have a chance to get to know our kids and our neighbors’ kids, know what they’re doing when you’re not looking, and know what wonderful resources there are online.

Ask them to set up a program to try to get parents involved. Do what you can to help; they deserve our support and admiration. (I’ve said it before—librarians are our most underestimated natural resource. And I’ve been lucky enough to know some really sensational ones.) Try and get parents to contribute meaningfully to the plans to get your schools and libraries online, safely. Share the wealth. Convince parent volunteers to teach you what they know. Have them look over the school’s proposed acceptable-use policies and see if there’s something they can suggest to improve them. See if you can get them to volunteer to help teach other parents and share resources and sites you’ve found. Hold hands-on workshops, using the school technology center to show them how to turn a computer on and conduct a search. Share keywords (the words used in sites you want to filter or block) that you’ve discovered if they use filtering software. The only way we can truly protect our children in cyberspace is to build a solid team of parents, friends, librarians, and schools.

Appendix 1

FERPA The Family Educational Rights and Privacy Act of 1974 - (20 U.S.C. §1232g)

Introduction to FERPA

The Family Educational Rights and Privacy Act of 1974 (FERPA) (20 U.S.C. §1232g) was enacted to protect the privacy of students and their parents. It sets forth conditions for the receipt of federal funding by schools and universities as well as other educational institutions. Institutions can only receive these funds if they comply with a set of procedures for allowing students and families access to their educational records while at the same time limiting access to those records by other people and parties.

FERPA prevents schools from releasing personally identifiable information about a student. This personally identifiable information includes the student's name, the names of their parent(s) or guardian(s), the address of the student or their family, personal identifiers such as social security numbers, lists of personal characteristics that would make the student's identity easily traceable or any other information that would make the student's identity traceable. This includes dissemination by computer media, as well as any other recorded means of transmission.

ISchools are allowed to disclose "directory information"

FERPA does allow schools to disclose certain types of information on students. This includes information released pursuant to a subpoena in a court case, either civil or criminal, information released in response to mandatory government reports, information released to other educational institutions where th student plans to enroll, information released for the purposed of financial aid, etc. (34 C.F.R. §99.31)

Another class of information which schools are allowed to disclose is information specified as so called "directory information." This sort of information may be disclosed if the school has given public notice to parents of students in attendance and eligible students (those over age 18 or in postsecondary institutions) in attendance of the types of information designated as directory information, their right to refuse release of the information, and the procedure for notifying the school that they do not want some of all of their or their child's directory information released. (34 C.F.R §99.37)

The list of information which schools and institutions may designate as directory includes, but is not limited to:

the student's name, address, telephone listing, electronic mail address, photograph, date and place of birth, major field of study, dates of attendance, grade level, enrollment status (e.g., undergraduate or graduate; full-time or part-time), participation in officially recognized activities and sports, weight and height of members of athletic teams, degrees, honors and awards received, and the most recent educational agency or institution attended. (20 U.S.C. §1232g(a)(5)(A)).

Once designated as directory information, and proper notice has been given, schools may release this information without seeking permission from parents, guardians or eligible students. Information on students no longer in attendance may be disclosed without meeting any of the formal requirements of this definition or 34 C.F.R. §99.37(a).

Notice requirements

"Each educational agency or institution shall *annually* notify parents of students currently in attendance, or eligible students in attendance, of their rights under [FERPA]." (34 C.F.R. §99.7) For directory information, this notice must include, among other things:

1. The types of information designated as directory information;
2. The fact that the parent or eligible student has the right to object to the release of some or all of this personal directory information; and
3. The period of time in which a parent of an eligible student has to notify the agency or institution in writing that they do not want this information released as directory information.

This notice must be made public. Publication in a school newsletter, student handbook, or similar publication. In elementary or secondary schools, the notice must effectively notify parents, guardians and eligible students of these rights in multiple languages if the situations at the school warrant. (34 C.F.R. §99.7(b)(2)).

For information other than so called directory information, prior consent of the parent, guardian or eligible student is required before the institution may release personally identifiable information from the student's records. This consent must specify the information to be disclosed, the purpose for the disclosure, and identify the party or class of parties to whom the disclosure can be made. (34 C.F.R. §99.30) Furthermore, if the parent or student so requests, the school or institution must provide them with a copy of the information actually disclosed to the authorized third party.

If notice is not provided for disclosure of directory information, or information is released without proper consent for all other information, than the school or institution releasing the information runs the risk of forfeiting all federal funding to which they would otherwise be entitled.

Recording requirements

In addition to ensuring that information is released properly and only when appropriate, the school, agency or other institution must also be sure to maintain proper records of who requests access to personally identifiable student information as well as all parties to whom authorized information is released. (34 C.F.R. §99.32)

This record must include the parties who have requested information, the legitimate interest they had in making the request as well as the names of the additional parties to which the receiving party may disclose the information, and the legitimate interest each of these additional parties may have in the student information. The record of these requests shall be maintained with the educational records requested and shall remain a part of those records for as long as the records themselves are maintained.

The recording requirement does not apply, however, to requests made by or disclosures to the parent or eligible student, a school official, a party seeking directory information, or a party seeking information as directed by a grand jury or other law enforcement subpoena.

Duties of parties to whom information is disclosed

Any information released by a school or other institution to any third party is released on the condition that the party to whom the information is disclosed will not disclose that information to any other party without obtaining the consent of the parent or eligible student. Officers and employees of the party to whom the information is released may only use that information for the purposed for which the disclosure was made.

Information disclosed under FERPA to third parties may only be re-disclosed if specific conditions are met. The further disclosures must:

1. Meet the requirements of 34 C.F.R. §99.31 (all the releases an institution may make without prior written consent of the parent, guardian or eligible student. This is basically the opt-out scheme related to directory information); and
2. The educational institution must have complied with the requirements of 34 C.F.R. §99.32(b) (requiring that the school keep a proper written record of each request for access to and each release of personally identifiable information).

Conflicts with state laws

If any requirement of FERPA is believed to be in conflict with a state privacy law, the agency or institution seeking to withhold the student's information is supposed to notify the Office of the Secretary of the Department of Education within 45 days giving the text and citation of the conflicting law. (34 C.F.R. §99.61)

Questions remain as to what remedies are available to private parties aggrieved by alleged violations of FERPA. under the statute, enforcement is handled by the Department of Education, but the administrative remedies set forth there have been criticized as inadequate. Violations may result in institutions losing money, but it does not correct for the release of the private information or provide for any damages to those injured. The only way this can be accomplished is through a private action under 42 U.S.C. §1983. It seems that not all administrative remedies need be exhausted before this action is brought, and this action does appear to allow individuals to obtain relief against individual defendants found to be in violation of the requirements of FERPA.

Appendix 2

How Safe are Your Kids Online at School?

(a handout for parents)
By Parry Aftab, executive director, WiredSafety.org

You've read my book on protecting your children online. You supervise your child's online activities at home. Your children know they can come to you when things go wrong online. You set rules and enforce them. No chat, no instant messaging people you haven't approved, no one on their buddy list you don't know in real life, no filling out registration forms, no profiles or personal information on their websites. That keeps them safe until they leave for school and someone else sets the rules (if they have rules at all). Should you worry about school Internet access? How safe are your children online at school?

Statistically, they are safer online at school than they are surfing at home. This is due to several important factors. To begin with, children are generally better supervised at school. Someone is usually overseeing their entire online activities, either by setting the monitors where they can see them, or through the use of parental control and monitoring technologies. In addition, most children have limited Internet access at school. This is a big factor in keeping them safe. Studies we have conducted at WiredKids.org disclose that the more time children spend online, the more likely they are to engage in high risk activities, such as conversing with strangers, giving out personal information and having cybersex discussions. The students don't have enough time online at school to get into these things, generally.

Another important factor is the expertise of school librarians and (if your school is lucky enough to have one) library-media specialists. No one knows more about the good, the bad and the ugly online than these underappreciated miracle workers. They can usually predict which students will get into trouble and how. One library-media specialist told me that you can always tell when a student is surfing where they shouldn't be – all the other students are crowding around them trying to see what's on the screen. And, she also told me that this is rarely pornography. It is far more often a gory site, with baby seals being clubbed to death or something equally offensive or a site that targets another student at the school. Together with the technology team at the school, the librarians and library-media specialists can usually find the sites that cyber-bully students. They just watch for high traffic to little known sites. (Students always flock to the sites they heard about at school.)

Many schools also block access to instant messaging services, and chat. Since most Internet sexual predators groom the children using either instant messaging or chat, this alone makes your child much safer online. But there are still risks and you should be sure your school is doing something about minimizing those risks. And there are also special risks specific to school Internet use. Find out how your school is addressing those as well.

Start by asking if the school has an acceptable use policy. The policy should be signed by both the student and the parents. It should articulate the rules about what is permitted and what is prohibited. It should also let the students know where to report problems they encounter and the consequences of violating the acceptable use policy. Find out what happens if a parent refuses to sign the policy. Too many schools allow the student to access the Internet anyway, feeling that it is needed for their education. The school should, however, treat it the same way they would treat a permission slip for a school outing. No slip, no trip. No signed policy (without modifications!), no Internet access. If the school stands firm on this, most parents will come around.

Next ask about privacy. Does the school have a website? Is any personal information about the students posted there? Has the school directory been posted online? What about the team rosters? Any student photos at the website? If so, are they in larger groups, or in individual photos? (I advise schools to only use photos with groups of four or more students, and only identify them by class or club, rather than by name.) Does the school permit students to fill out forms online or register at websites? In addition to general privacy and security concerns, COPPA (The Children's Privacy Protection Act) prohibits websites from permitting the use of any interactive communication technology (chat, instant messaging, discussion boards, e-mail) by preteens or from collecting personally-identifiable information from children under the age of thirteen without the parents' permission. While there are exceptions allowing schools to act in lieu of a parent in giving this consent, has the school informed the parents about this? Are the teachers even aware that they are acting in special legal capacity when they allow students to fill out forms or use interactive communication tools online? Do they even know about COPPA?

What if some students decide to cyber-bully another? Has the school had to deal with cyber-bullying and harassment previously? How did they handle it? Often schools try to discipline the student for websites and online communications originating from home. But in every case when the discipline is challenged, the school loses. Some schools have had to pay substantial damages in lawsuit brought on behalf of the student by the ACLU and other civil liberty groups. The school should be calling in the students and resolving this consensually, with the parents' involvement.

Online threats, where a student receives a death threat, or threat of bodily harm, or when a bomb-threat or similar warning is encountered, law enforcement must be called immediately. This is not a time for the school to try and handle this without the assistance of outside law enforcement agencies. The Littleton, Colorado attacks were foretold online. Many other attacks have been avoided by the swift action by the school administration and local law enforcement officers. Ask the school if they have a school safety officer, or if they know who to call at the law enforcement agency if something serious occurs.

Has the technology team discussed how to preserve the cyber-evidence and retain any logs? Do they know what to do with them once preserved? The time to find out is now, not in the middle of a crisis. Ask your local law enforcement agency to send one of their cyber-detectives over to visit the school. If they don’t have anyone with this expertise, they can reach out to the nearest ICAC task force unit (Internet Crimes Against Children) for help. (ICACs are units of Federal, state and local law enforcement agents formed by the Department of Justice and trained to work together to prevent and investigate Internet crimes against children.) The technology team may want to consider installing a monitoring product, such as Spectorsoft Pro, to make sure that all activity is collected and stored. This can be a God-send when something serious occurs and you need to find out quickly what happened. (Just make sure the school notifies parents and students in the acceptable use policy of the use of any monitoring product.)

Federal Law: When Websites Collect Information About Students under the Age of 13 or Allow Students under the Age of 13 to Post Personal Information

COPPA DEVELOPMENT AND ANALYSIS

The Children's Online Privacy Protection Act ("COPPA"), and the regulations thereunder which took effect on April 21, 2000, require all commercial sites to take special measures when they collect personal information from children or allow children to use interactive features, such as e-mail, instant messaging and chat (if they could share personal information with others using those tools). Many sites are confused about what the law provides, since it uses the word "collection" and they see that as something affirmative they are doing. But "collection" includes letting children use e-mail accounts or post messages publicly through a chat room or discussion board, as well as fill out forms. And it has nothing to do with adult content children may see online.

While the regulations are aimed principally at the children's Internet industry, they are fully effective against general interest sites with actual knowledge that a child is using their services. Few lawyers, even among experienced cyberspace practitioners, understand the children's Internet industry and the regulations and safety concerns that apply to it. But failing to understand what information can be collected from children, how it can be used, and what must be accurately disclosed to parents has cost many companies dearly.

Schools acting in parental roles or as a parent's agent for the purposes of granting consent are often finding themselves used by commercial websites to give the consent the sites cannot get from parents. And teachers often have no idea that they are providing a way around the law. The more they understand about how COPPA works, and the care they should take to get parents' approval, the safer a school will be, legally.

There are two issues dealt with by COPPA and the existing consumer protection authority of the FTC. One is privacy, the other is safety. Both are regulated by the FTC, although states are permitted to enforce consistent local laws. In brief, privacy relates to the collection, maintenance, or use of personally identifiable information from children 12 years old and under. Safety is impacted, legally, when a child under the age of 13 is able to share personally identifiable information with others online.

The safety concern is that someone such as a pedophile may be able to contact the child either online or offline because the child has shared such contact information, whether intentionally or not. Last October, the FTC promulgated its final regulations implementing the Children's Online Privacy Protection Act of 1998 (COPPA). Yet few were aware that the FTC already had the ability to enforce the privacy and safety concerns noted above, and has expressly set forth the parameters of that authority since mid-1997.

The salient document is the " Kids-Com Letter." Online since February 1995, KidsCom was one of the first children-only sites on the Internet. It did not use "cookies"-which glean data about site visitors-to gather information, but collected data through registration forms, contests, and pen pal programs. It was directed at children from ages four to 15 and came under criticism for its collection practices. (As a result of the FTC investigation, KidsCom revamped its site and is very popular among parents and children.)

In May 1996, the Center for Media Education, a consumer watchdog group, filed a petition with the FTC requesting that the agency investigate KidsCom and bring an enforcement action against it. CME asserted that KidsCom's data collection practices violated Section5 of the FTC Act's "anti-deception" laws in two ways. First, KidsCom collected information from children without accurately disclosing the purpose, and second, KidsCom failed to disclose that it was paid to endorse certain products. In July 1997, the FTC issued its findings in a letter. The FTC determined that KidsCom's disclosure was "likely" inadequate and misleading, but declined to take any punitive action against KidsCom since the company had already changed its data collection practices and cooperated in the FTC investigation. The FTC discovered that KidsCom was sharing information collected from children with third parties, though this information was provided only in an aggregate form (e.g., 10-year-old boys from New York preferred baseball over football).

In issuing this ruling, the FTC for the first time publicly announced its guidelines for data collection from children on the Internet. Relying on '5 of the FTC Act, which prohibits unfair and deceptive practices in or affecting commerce, the FTC stated: "It is a deceptive practice to represent that a Web site is collecting personally identifiable information from a child for a particular purpose (e.g., to earn points to redeem a premium), when the information will also be used for another purpose which parents would find material, in the absence of a clear and prominent disclosure to that effect."

Second, the FTC stated, when collecting personally identifiable information, "adequate notice" of such practices must be given to a parent because of a child's limited ability to understand the disclosure. "Adequate notice" requires disclosure of: (1) who is collecting the personally identifiable information; (2) what information is being used and for what purpose it is being used; (3) whether it will be disclosed to third parties, and if so, to whom and in what form; and (4) how parents can prevent the "retention, use or disclosure" of that information.

Third, the FTC articulated its "unfairness" test for Internet child safety, noting that the disclosure of children's personal information to third parties is of particular concern, and that parents must be given adequate notice of such use and the opportunity to deny their consent to it. The FTC has had broad regulatory powers when dealing with safety issues, under its unfairness authority in section 5. Under that section, a practice is unfair if it causes or is likely to cause substantial injury to consumers that is not reasonably avoidable and not outweighed by countervailing benefits to consumers or competition.

In its fourth and final principle, the FTC criticized KidsCom's endorsement practices as misleading and deceptive. KidsCom had "New Product" areas, where products were reviewed and endorsed. What it had not disclosed was the fact that, in exchange for an endorsement, product manufacturers had to contribute at least $ 1,000 worth of product, which was used for premiums and prize redemptions. The passing off of an advertisement as an independent review or endorsement is a deceptive practice under '5 of the FTC Act. KidsCom failed to clearly and conspicuously disclose that the product information was solicited from manufacturers and printed in exchange for in-kind payment.

Following the issuance of the KidsCom Letter, the FTC broadened its principles to include offline consent for children 12 and younger anytime their personal information may be shared online in chat rooms or similar third-party communications, and before any site collects and stores their personal information, even an e-mail address.

The adoption of COPPA was in direct response to the lack of industry compliance with the law as articulated by the FTC in the KidsCom Letter.

In June 1998, the FTC presented its Privacy Online Report to Congress, documenting the online collection of personal information from children. The FTC rearticulated its prior concerns that collection of personal information from a child under the age of 13 without informed parental consent would be a deceptive trade practice. The FTC reported to Congress that even in chat rooms, children innocently and without request may reveal where they live or go to school or their real e-mail addresses. The FTC informed Congress that parents need to understand the risks and consent to any such collection and disclosure of personal information. Congress apparently agreed, and wasted no time in acting on the FTC's report. Within months, COPPA was law.

COPPA requires that commercial Web sites obtain verifiable parental consent before collecting personal information from a child under the age of 13. Failure to obtain such consent is an unfair and deceptive trade practice and can result in fines of up to $11,000 per occurrence.

COPPA applies to commercial Web sites, online services "targeted at children," and any online service operators with actual knowledge that they collect personal information from a child. (Actual knowledge can be as simple as a child's sharing her grade or age in a monitored general audience chat room on a site, or can be supplied by an e-mail or phone call from concerned parents who object to the collection practices on behalf of their child.) Personal information includes such items as full name, home address, e-mail address, telephone number, Social Security number, or any other information that the FTC determines "permits the physical or online contacting of a specific individual."

The regulations require covered operators to:

1. Provide notice on the Web site of what information is collected from children, how information is used, and the Web site operator's disclosure practices for such information (notice this applies to all information, not just "personal information");

2. Obtain verifiable parental consent (which requires more than a mere e- mail consent from the parent) to collect, use, or disclose children's personal information before it is collected from the child, with certain exceptions and special rules for newsletters and internally used information;

3. Upon request, provide parents with a description of the types of information collected from their child, or the actual information obtained from their child, and the opportunity to refuse to permit the further use, maintenance, or future collection of the child's personal information. Thus, in addition to having to obtain initial consent from the parents, if a parent withdraws consent at any time, the operator must remove that child's personal information from the system;

4. Cease conditioning the child's participation in games, contests, or any other activity upon the disclosure of more information than is reasonably necessary to participate, including permitting parents to allow the site to collect personal information but refusing to let the site share the information with third parties;

5. Maintain reasonable procedures "to protect the confidentiality, security, and integrity of personal information collected from children."

The law also details three different levels of consent, as well as the various types of notices required under the statute, which cover everything from the content of those rules to the look and placement of the link to the privacy policy displayed at the site, as well as the technical requirements for obtaining "verifiable" parental consent.

All websites need to look hard and thoroughly at their collection practices. Even if COPPA doesn't apply to the site, they may still run afoul of the FTC Act if their privacy policy does not accurately and completely disclose what personal information they collect from their users and what they do with that information. If they collect personal information that includes a person's age or grade or similar information, they may then have actual knowledge that they are collecting personal information from a "child" and need to comply with the full panoply of COPPA regulations. Even if they don't overtly request that information, if they have monitored chat rooms or discussion boards at which a user may disclose information from which the site should know they are under 13, that may provide the requisite knowledge under COPPA.

If the site collects any personally identifiable information from its users or provides any means of public disclosure of such information (such as through an e-mail service, chat room, discussion boards or instant messenger service), and the site is alerted that a particular user is a statutory "child," then the site must also comply with COPPA.

Banner advertisers and network advertising companies are covered by COPPA and its regulation if they advertise at children's sites and collect personal information from children who click through from such sites. They are also covered if they have ownership or control over such information collected directly at the children's sites. Advertisers at general audience sites may also be covered by COPPA if they collect personal information from people who click through, and that information discloses that the visitor is a child.

We have learned that many companies are collecting data from their Web site visitors without knowing why they are collecting it or if they are using it properly. Unless companies are under investigation or have heard of another company under investigation, their legal departments rarely communicate with Webmasters. With this new law on the books, all commercial Web sites must be vigilant in ensuring that the rights of parents to notice and consent are honored. If such companies ignore parents' concerns regarding privacy and advertising, they will have to face more than the FTC they will be facing the even tougher scrutiny of a disgruntled parent.

Appendix

Cyberbullying Guide:

What’s the difference between rude communications and cyberbullying/harassment?: Telling the difference between flaming, cyber-bullying and harassment and cyberstalking

It’s not always easy to tell these apart, except for serious cases of cyberstalking, when you “know it when you see it.” And the only difference between “cyberbullying” and cyber-harassment is the age of both the victim and the perpetrator. They both have to be under-age in a cyberbullying case. Schools needs to know when to get law enforcement involved and how to spot the real dangers as opposed to the merely hurtful communications. When analyzing a communication, consider the following:

The kind of threat:

- The communication uses lewd language
- The communication insults your child directly (“You are stupid!”)
- The communication threatens your child vaguely (“I’m going to get you!”)
- The communication threatens your child with bodily harm. (“I’m going to beat you up!”)
- There is a general serious threat. (“There is a bomb in the school!” or “Don’t take the school bus today!”)
- The communication threatens your child with serious bodily harm or death (“I am going to break your legs!” or “I am going to kill you!”)

The frequency of the threats:

- It is a one-time communication
- The communication is repeated in the same or different ways
- The communications are increasing
- Third-parties are joining in and communications are now being received from (what appears to be) additional people

The source of the threats:

- Your child knows who is doing this
- Your child thinks they know who is doing this
- Your child has no idea who is doing this
- The messages appear to be from several different people

The nature of the threats:

- Repeated e-mails or IMs
- Following the child around online, into chatrooms, favorite websites, etc.

- Building fake profiles, websites or posing as your child’s e-mail or IM
- Planting statements to provoke third-party stalking and harassment
- Signing your child up for porn sites and e-mailing lists and junk e-mail and IM.
- Breaking in to their accounts online
- Stealing or otherwise accessing their passwords
- Posting images of the child online (taken from any source, including video and photo phones)
- Posting real or doctored sexual images of the child online
- Sharing personal information about the child
- Sharing intimate information about the child (sexual, special problems, etc.)
- Sharing contact information about the child coupled with a sexual solicitation (“for a good time call …” or “I am interested in [fill in the blank] sex…”)
- Reporting the child for real or provoked terms of service violations (“notify wars” or “warning wars”)
- Encouraging that others share their top ten “hit lists,” or ugly lists, or slut lists online and including your child on that list.
- Posting and encouraging others to post nasty comments on your child’s blog.
- Hacking your child’s computer and sending your child malicious codes.
- Sending threats to others (like the president of the United States) or attacking others while posing as your child.
- Copying others on your child’s private e-mail and IM communications.
- Posting bad reviews or feedback on your child without cause.
- Registering your child’s name and setting up a bash website or profile.
- Posting rude or provocative comments while posing as your child (such as insulting racial minorities at a website devoted to that racial minority).
- Sending SPAM or malware to others while posing as your child.
- Breaking the rules of a website or service while posing as your child.
- Setting up a vote for site (like “hot or not?”) designed to embarrass or humiliate your child.
- Masquerading as your child for any purpose.
- Posting your child’s text-messaging address or cell phone number online to encourage abuse and increase your child’s text-messaging or cell phone charges.
- Launching a denial of service attack on your child’s website.
- Sending “jokes” about your child to others or mailing lists.

The more repeated the communications are, the greater the threats (or enlarging this to include third-parties) and the more dangerous the methods, the more likely law enforcement or legal process needs to be used. If personal contact information is being shared online, this must be treated very seriously.

If the child thinks they know who is doing this, that may either make this more serious, or less. But once third-parties are involved (hate groups, sexually-deviant groups, etc.) it makes no difference if the person who started this is a young seven year old doing it for a laugh. It escalates quickly and can be dangerous.

Appendix

Cyberbullying Guide

A quick guide for parents on the escalating levels of response to a cyberbullying incident:

Talk to your child: Caution them about responding “in kind.” This is not a time for them to lash out or start a cyberwar themselves. See if they think they know the identity of the cyberbully or cyberbullies. See if this is related to an offline bullying situation, and deal with that quickly. And don’t confuse the language most kids use online with cyberbullying. It may be shocking to us, but unless it is shocking to your child, it’s not cyberbullying.

Ignore it: A one time, seemingly unthreatening act, like a prank or mild teasing should probably be ignored. (If it’s a threat, you must report it.) At the same time, you may want to consider using some preventive measures:

Restrict the people who can send you communications: Consider restricting all incoming communications to pre-approved senders, such as those on your child’s buddy list. (If the cyberbully is someone on their buddy list, though, this method won’t help. In that case the cyberbully will have to be removed from the buddy list and/or blocked.)

Restrict others from being able to add your child to their buddy list: Cyberbullies track when your child is online by using buddy lists, and similar tracking programs. It will let them know when one of their “buddies” is online, when they are inactive and, in some cases, where they are. This is like adding a tracking device to your child’s online ankle, allowing their cyberbullies to find them more easily and target them more effectively. This feature is usually found in the privacy settings or parental controls of a communications program.

Google Your Child: Make sure that the cyberbully isn’t posting attacks online. When you get an early warning of a cyberbullying campaign, it is essential that you keep an eye on your child’s screen name, nick names, full name, address, telephone and cell numbers and websites. You can also set up an “alert” on Google to notify you whenever anything about your child is posted online. To learn more about “Googling” yourself or your child, read “Google Yourself!”

Block the sender: Someone who seems aggressive, or makes you uncomfortable and does not respond to verbal please or formal warnings should be blocked. This way, they will not be able to know when you are online or be able to contact you through instant messaging.

Even if the communicates are not particularly aggressive or threatening, if they are annoying or, block the sender. (Most ISPs and instant messaging programs have a blocking feature to allow you to prevent the sender from getting through.)

"Warn" the sender: If the cyberbully uses another screen name to avoid the block**,** otherwise manages to get through or around the block or communicates through others, "warn" them, or "notify" the ISP. (This is usually a button on the IM application.) This creates a record of the incident for later review, and if the person is warned enough, they can lose their ISP or instant messenger account. (Unfortunately, many cyberbullies use "warning wars" or "notify wars" to harass their victims, by making it appear the victim is really the cyberbully. This is a method of cyberbullying by proxy, getting the ISP to be an unwitting accomplice of the cyberbullying.)

Report to ISP: Most cyberbullying and harassment incidents violate the ISP's terms of service. These are typically called a "TOS violation" (for a "terms of service" violation, and can have serious consequences for the account holder. Many ISPs will close a cyberbully's account (which will also close their parents' household account in most cases.) You should report this to the sender's ISP, not yours. (For more information about how to make a report, read "Making a Report to Their ISP." If you use a monitoring software, like Spectorsoft, this is much easier.)

If your child's account has been hacked or their password compromised, or if someone is posing as your child, you should make a formal report to *your* ISP as well. You can call them or send an e-mail to their security department (NOT their terms of service reportline). But before changing your password, you should scan your computer for any hacking programs or spyware, such as a Trojan horse. If one is on your computer, the cyberbully may be able to access the new password. Most good anti-virus programs can find and remove a hacking program. All spyware applications can. We recommend SpyBot Search and Destroy (a freeware) or Ad-Aware (by Lavasoft, they have a free "lite" program).

Report to School: Most cases of cyberbullying occur off school grounds and outside of school hours. In the United States, often the school has no legal authority to take action relating to an off-premises and off-hours activity, even if it has an impact on the welfare of their students. The laws are tricky, and vary jurisdiction by jurisdiction. So while you should notify the school (especially if your child suspects whom is behind the attacks), they may not be able to take disciplinary action. They can keep any eye on the situation in school, however. And since many cyberbullying incidents are combined with offline bullying incidents, your child may be safer because of the report.

Also, while the school may have limited authority over disciplining the cyberbully, they can call the parents in and try and mediate the situation. They can also institute an educational and awareness program to help stop further cyberbullying by students, and to help educate parents about the problem. Schools can also set up anonymous tipline, so students can report cyberbullying the moment it starts.

Report to Police: Someone who threatens you physically, who is posting details about your or your child's offline contact information or instigating a cyberbullying by proxy campaign should be reported to the police. (Although you should err on the side of caution and report anything that worries you.) Using a monitoring program, such as Spectorsoft, can facilitate the investigation and any eventual prosecution by collecting and preserving electronic evidence. Print-outs, while helpful in explaining the situation, are generally not admissible evidence.) If you feel like your child, you or someone you know is in danger, contact the police immediately and cut off contact with this person or user, staying offline if need be until you are otherwise instructed. Do not install any programs, or remove any programs or take other remedial action on your computer or communication device during this process. It may adversely affect the investigation and any eventual prosecution.

Take Legal Action: Many cases of cyberbullying (like their adult cyber-harassment equivalent) are not criminal. They may come close to violating the law, but may not cross the line. Most of the time, the threat of closing their ISP or instant messaging account is enough to make things stop. But sometimes, either because the parents want to make an example of the cyberbully or because it isn't stopping, lawyers need to be brought in. It may also be the only way you can find out whom is behind the attacks.

Think carefully before you decide to take this kind of action. Even if you win in the end, it may take you two or three years to get there and cost you tens of thousands of dollars. You may be angry enough to start it, but make sure that you have something more than anger to sustain the long months and years of litigation.

Appendix

Ms. Parry's Guide to Correct Online Manner (Netiquette):

A Checklist for Cyber-communications (thinkb4uthink) written for students:

Before sending that e-mail or posting on that website or bulletin board, think before you click "send." Re-read what you were going to send. If it meets any of these factors, don't send it until you fix them. And if you can't fix them, maybe you shouldn't send it at all.

It's so easy for anyone to misunderstand e-mails and cyber-communications. We have to be very, very careful to make them clear and help others to understand what we really mean. We also need to be careful not to hurt others and be good netizens.

- **Start by making sure you are sending things to the right place, that it arrives and that the right person gets it.**

  Is it addressed to the right person? Are you sure? Have you checked the spelling and the screen name carefully? Are they in your address book or on your buddy list already? The easiest way to make sure that you have their correct screen name or e-mail address is to save it automatically when they send you something. Parents should input their children's approved correspondents into their buddy lists and address books to make sure that it is done correctly. Also, people (especially kids) change their e-mail addresses and screen names often. Make sure you are using the most up-to-date one.

  Also, don't be so sure that your e-mail makes it to the person you sent it to. With so many junk e-mails and viruses being sent these days, most Internet service providers are using SPAM-blocking technology to block and filter messages they think may be SPAM. Many innocent messages are caught in the SPAM-filters and never get delivered anymore. Some people are also using their own anti-SPAM software that may block your e-mail. Remind your friends to add your e-mail address and screen name to their approved list so that you won't be blocked by accident and warn them in advance before using a new address or screen name. Depending on which e-mail service you use, you may be able to track your message and see if it is ever delivered, and sometimes if it is even read. There are other applications you can use as well. It's good netiquette to ask the person before sending something to track whether they have opened or read the e-mail before using it. But just because you send something, don't get angry if the other person doesn't reply. First make sure they received it. (And make sure that they aren't blocked by your e-mail filters or SPAM-blockers either.)

Sometimes one family will use the same e-mail address or screen name for everyone. It could be embarrassing if you send a personal and private message to someone and their parents or older brother reads it instead. Check first. Also, many parents read their kids e-mails. Check with your friends and see if their e-mails are reviewed by their parents. You may want to be more careful if they do.

- **Is it worth sending? Don't waste peoples' time or bandwidth with junk, chain e-mails and false rumors**

Some of your friends and people you know love getting lots of e-mail, IMs and jokes. Others don't. Before you start sending lots of jokes and attachments to someone, find out if it's okay first. And if they tell you they are busy, respect their time. It never hurts to ask first. That way people will look forward to getting your e-mails and cyber-communications instead of ignoring them. Also, don't send long e-mails to people who only read short ones, or short ones to people who like long ones without explaining why.

Don't send chain e-mails. They clog up e-mail servers, especially at school. And sometimes scare people, especially younger kids. Also, sometimes bad people who are looking to find kids online use them to spy on e-mails and find new kids to contact. (You can read more about chain e-mails at "e-mail netiquette and safety.")

Also, never send anything you haven't confirmed as being true. Many hoaxes and cyber-rumors are sent by people who just blindly forwarded them on, without checking to see if they are true. (You can read more about urban legends, hoaxes and cyber-rumors and how to check and see if they are true or not at our "Truth or Hype" section.)

If you are going to send an e-mail to someone famous you found online, think about what you're going to say. Many of these people answer select e-mails, and you want yours to be answered, not ignored. Also, if you ask them for something that is inappropriate (like helping you write your term paper) or something you should have found on your own (like their biography or information readily found at their website) they probably won't bother answering you.
Also, don't just send a "hi!" message without more. The worse that will happen is that it will be caught in the SPAM-filter or ignored. The best that will happen is that they will say "hi" back. What good is that? Also, never send an attachment to someone you don't know. They will probably automatically delete it. You can almost always include a photo or the document in the e-mail itself, instead of having to attach it. And make sure that you have allowed them to reply, without finding that they are blocked by parental controls or your e-mail filters.

- **Proofread and spell-check your e-mails and make sure they know who you are**

Many messages are never understood or are misunderstood because people left out words, or said things unclearly, or misspelled words. While your e-mails don't have to be formal works of art, your should make them clear. If they are important enough to send, they are important enough to be understood. The rules for instant messaging are different and more grammar mistakes and spelling errors are accepted there.

Also make sure that you re-read what you are sending to make sure it says what you want it to say. If something could be misunderstood, or understood two different ways, either re-write it or use an emoticon to let them know which meaning you used. Don't use shorthands or acronyms they don't understand. And if you are referring to someone else, make sure they know who you are talking about.

Also make sure that you sign your e-mails and cyber-communications with a name the recipient will recognize, if you aren't using your normal screen name. Don't' give away personal information, but telling them that this is a new account or screen name and your old one was [fill in the blank] helps your message get read, instead of trashed. Putting that in the subject line may help.

- **Don't attack others online, say anything that could be considered insulting or that is controversial**

Until you get to know someone very well, it's always best to stay away from controversial topics, like politics, religion, race, sex, nationalism, war, special physical or mental limitations, money and gender-based issues. Once you get to know each other well-enough to know what is acceptable, you can get into these topics online, but even then, be very careful. Most cyber-problems start when people are talking about these and similar topics.

And be especially careful when dealing with people form other cultures and countries online. What may be perfectly acceptable in the United States may not be acceptable in Japan, or England, or Hong Kong, or New Zealand. Watch what they say and how they say it before jumping in. Be extra polite and respectful and don't be afraid to ask how they do things where they live. It's a great way to learn.

If someone tells you that you hurt their feelings, find out how and apologize. Let them know when you did things without meaning to. If they lash out at you, thinking you did it on purpose, before you attack them back, try explaining that it was accidental.

Don't use all capital letters (considered shouting online) and be careful about using bad language or being provocative. Don't intentionally say anything to hurt some else's feelings or invade their privacy online or offline. And always scan your system for viruses and malicious code so that you don't send a virus by accident to someone else. (Use a good anti-virus program on anything you receive or download to make sure you don't pick up any viruses.)

- **Don't forward other people's e-mails without their permission or share their personal information**

  Sometimes, without realizing it, we copy someone new on an e-mail thread. It might contain personal information or a personal communication that someone else shared with only you three levels down and you didn't realize that you were now allowing others to read it. Either delete all but the most recent message when forwarding it, or re-read the older threaded messages before forwarding to make sure nothing personal is in those messages. Many private things slip through that way by mistake.

- **Are you angry when you are writing this message?**

  If you are writing the e-mail, instant message or post when you are angry, review it carefully. Also take the time to cool down before sending it and check the tips for avoiding cyberfights, by using the tips we learn in Take 5!

  Are you replying to something that is designed to insult you, flame you, cyber-bully you or harass you? If so, think again. These things go away much faster if you don't reply at all. The person sending them is looking for a reaction. They soon get tired and go away if they don't get any. Also, you should let your parents or teachers know if you are receiving hateful or threatening cyber-communications or if you receive something that hurts your feelings or makes you feel bad. You are entitled not to be attacked online and enjoy e-mail and cyber-communications without worrying about nasty people.

- **Don't reply to SPAM, even to ask to be removed from their mailing list**

  SPAMMers buy lists of millions of e-mail addresses and instant messaging screen names. Harvesting programs gather up these addresses wherever they can find them online, in chatrooms, on message boards, from chain e-mails and registrations. So, many of these addresses are old and don't work. If you reply, one of two things happens. You either have sent a reply to a fake address they have used to send the e-mails from, or you have now let them know that your address is a good one and you will receive many more messages. They will even sell your address for more money, since they can now promise that you have read the SPAM messages you receive.

  While your e-mail service provider may ask you to forward SPAM to their TOS (terms of service violations address), you shouldn't bother. Instead, use a good anti-SPAM program or the dual e-mail trick. [link to dual e-mail trick])

- **How private is the message you are sending? Are you willing to have others read this message or forward it to others without your permission?**

  E-mails get misdelivered all the time. And sometimes the people we send them to share our communications with others without asking us first. (This includes logs of our chatroom discussions and of instant messaging.) The courts allow others to read your e-mails under special circumstances. Don't ever say anything in a cyber-communication you wouldn't be willing to allow someone else to read. We always tell people not to say anything they wouldn't write on a postcard they send through the mail. Sometimes when our friends get angry with us, they intentionally post our e-mails on public websites or send them to others. If you are going to share something very private, it's best to use the phone or person-to-person communications (obviously only with people you know in real life).

When students apply for jobs or internships the recruiter will sometimes "Google them" first. We have seen many cases where old messages they posted when they were much younger and didn't realize would turn-up in an online search cost someone an internship position or a job. (It's always a good idea to "Google yourself" regularly and make sure nothing turns up that you would be embarrassed about or that gives away personal information about you online.)

Also, many parents and schools monitor communications. This means they can read what you have written. Have you written anything they can't read? And if you are using a family account that one of your parents uses for work e-mail, their boss may be monitoring e-mails too. That could be very embarrassing for everyone and may cost your parent their job.

Appendix

Blogs, personal websites and social-networking profiles (from my new book, Internet Safety 1-2-3! and written for parents)

What Children are Saying When You're Not Around

There are always trends in what kids are doing online. The latest trends are cyberbullying and posting their online diaries and most personal thoughts on social-networking websites. These sites include MySpace.com, Xanga.com and FaceBook.com, among others. They are a cross between an online diary, a cyberdating network and a place to share your creativity and express yourself – on steroids. ☺

Recently, I have been receiving a large number of inquiries from schools, parents, regulators and the media about social-networking websites. I decided that it was important to address parent and school concerns and answer their questions where they needed it most. So, we agreed to work with the most popular of all social-networking sites, MySpace.com. We will also be sharing our safety tips at the other leading sites, as well.

MySpace.com and other similar sites are designed to allow people to share their creativity, pictures, and information with others. It also allows them to network with others online. Sometimes people do this to find romance. Sometimes they do it to find friends with similar interests. While this may be okay for adults, it is not okay for kids and may not be okay for young teens without parental supervision.

Most social-networking websites agree and prohibit anyone under a certain age from using their website. Unfortunately, while they may set rules to keep younger teens off the site, they can't prevent kids from lying about their age and pretending to be old enough to use the website. (These sites are typically free and without a payment authentication, they never know who their members are in real life.) To address the lying some sites have developed special software applications designed to help identify underage members by reviewing the contents of member profiles. It's not perfect, but it does help spot many underage members.

While we can't always tell if someone is lying about their age, some really do try to keep them off their site. Many other similar sites do not. So, when allowing your child to use a social-networking website, even with your supervision, make sure it's a trustworthy one.

We have learned a great deal about why kids use these kinds of sites. Most use them for innocent purposes. They want to find their friends and communicate among larger groups than they can do via instant messaging. They can post something and know everyone in their class or group can read it at the same time. They want to show off their creativity and how special they are. And they can pretend to be prettier, more popular, richer and more famous than they are in real life.

Most aren't there for meeting strangers or checking out provocative photos. But in some rare cases, they are acting out, taking risks and seeking romance online. That's when things can get dangerous, of users of all ages, but especially young teens. (You can learn more about Internet sexual predators and how they operate at our new site for preventing and helping young victims of Internet sexual predators, Katiesplace.org.)

But there's more to it. When I polled more than 1000 kids every month on this, I learned that they love the creativity of it. They love expressing themselves so others can appreciate it. They enjoy adding sparkly graphics and sharing their stories, poems and jokes. One of the Teenangels (WiredSafety's expert teen and preteen program, teenangels.org) told me that it's all about "Pink! Pink! Pink!" She can build a page using pink font, on a black background and feel creative and cool.

As important as allowing them to express themselves in a creative way is, though, it's not enough to get me to do a turn-about with these kinds of sites and teens. I was very negative about these sites. I have now taken a second look after talking to another one of my Teenangels.

This Teenangel (a soft-spoken and gentle girl) did a research project on social networking websites. She reviewed some of these sites and listed the kinds of risks young teens face on these websites. She then went on to explain that she had several profiles online at these sites. I was initially shocked and disappointed that one of my expert teens would take such risks with their personal information when they knew better. When I asked her why she would do such a risky thing, as the Teenangels often do, this one taught me something new.

She explained that it's hard being a young teen these days. Few kids in the school will give you the chance to see how much you have to offer unless you are the captain of the cheerleading squad or of the debate team. A profile page that is open to the other students at your school gives you a chance to share the special things about yourself with them, and will help them get to know you better. It's about sharing your favorite movies and books, about sharing fun vacation memories and your dreams, it's about sharing how special you are. It's about helping you make friends in your school with people who appreciate you. It's not about strangers, it's about others in their class.

There is a real value to that. Whether it's by posting a profile page that is supervised by their parents, or building a website. It can be pink and sparkly, or thoughtful and inspiring. But it's all about who your teen is or who they want to be. It's a challenge to give them a place where they can express themselves while keeping them safe, protected from predators and from sharing too much private information online. But if you are willing to supervise what they are saying and doing on their profiles, I'm willing to help.

Lying on their pages is part of what this is all about ,too. They pretend to be older (and not just to get around the age restrictions), richer, more famous or more popular. Boys pretend to be girls and girls pretend to be boys. They may be tall blonde surfers from Malibu or live on a ranch in New Zealand. While this may not be a problem, some of their other kinds of pretending can be dangerous for teens in a public social network.

They may act tougher than they are in real life "rl," provoke other, or talk about getting drunk, or their sexuality. They may pose as someone they don't like, to cyberbully and harass them, or steal their identities. I have spent years protecting children from predatorial adults. I never thought I would be spending as much time as I am protecting them from each other.

But, they are using these sites by the millions. And their use will only grow. So, it's worth the effort to find out if your child is one of them. Start by asking them. Hopefully they will be honest with you. If they aren't or you suspect they may be lying, it doesn't hurt to check out the more popular ones yourself. Search for your child by e-mail address, name and school. While they often lie about their e-mail address (either creating a special free web-based one just for this, that you may not recognize, or by making one up) or their name, they NEVER lie about their school. That's the only way their friends can find them. If you discover that your child has one of these profiles (or several, which is very common) and is lying to you, you need to take action. This isn't about technology, it's about dishonesty and hiding something important from you. And it might be a good time to buy and install a monitoring product, to be able to find their other lies and their next social-networking website they are trying to keep you from seeing.

If they admit that they have a page and show it to you, review it carefully, without over-reacting. Keep an open mind. (And take 5! to keep from panicking!) Have they posed as someone older? Posted person images? Included their friends on their site or been included by their friends on their sites? Forget the language. It's what kids do online. Caution them, but don't judge them by the language they use online. If they are posting using chatlingo shorthand, you can visit Teenangels.org and use our chatlingo translator to see what they are saying.

Then you have two choices. You can have the site taken down, or you can supervise what they are posting and doing. It's important hat you help keep your child safe online, even if you may be shocked by what you find your child is saying behind your back. And be aware that these are important to them. They all do it, even if they shouldn't. So, it's possible that your young teen will rebel and just set up a page again, but hide it better this time. It may be better to work with them than prohibit the profiles altogether.

Next, don't panic. You should take advantage of this opportunity to review their page first. You might be surprised (hopefully pleasantly) by what they are saying.

If they haven't posted anything to put them at risk, and aren't communicating with strangers, ask them why they want a social-networking profile page. You might be surprised at what they tell you. While parents freak out (understandably) at the provocative images and wild language used by many on these sites, most of the teens don't see them or pay attention to them. They are there to show off their creativity and self-expression and to communicate with their offline friends. As long as they are old enough to understand the rules and adhere to them (no one under 13 is old enough for this, even with parental approval in my humble opinion), and as long as you keep an eye on what they are doing, posting and how they are communicating with others, it's YOUR choice as to whether they keep their site up or not. (Make sure that you don't become the self-appointed profile site, reporting other people's kids for posting underage until you speak with their parents first!)

If you find that they are saying and posting inappropriate things or those comments don't seem to conform to their otherwise good offline behavior, don't panic yet. Think about how our parents would have reacted if they could have seen or heard everything we said to our friends when no adult was around. I guarantee that they would have been almost as shocked as many parents are about what their kids are posting online.

Also, remember that many of the things your kids are saying are being said to impress their audience and are often not true. (Luckily!)

The important difference between what we used to say or do and their posting online, however, is that when we acted out or boasted about acting out, we didn't do it to an audience of millions of people. So, while you shouldn't panic, you should take quick action if your kids are posting personal information in a public forum, or communicating with strangers online.

Also, know that this isn't new. Our kids have been saying and doing outrageous things online since the Web was born. We just don't know about it, but all the other kids do. It's how they communicate online. In 1999 we conducted the largest academic survey done to date for teenage girls. Almost 11,000 of the teens polled answered our questions about what they did online. When we asked them to explain if they had done anything online that they wouldn't have done in person, here's what they said (in their own words):

- "Yes, obviously people are more bold and outgoing on the Internet when they don't have to deal with the consequences of their actions."
- "Of course! All people do. A computer with a phone line is like a mask to the world. You can do or say anything and you won't ever have to meet this person. For instance, my little brother is 13 and he tells people he's 16 or older. He's a sweet guy and has a very high respect for females. Online, however, he says very cruel and suggestive things to and about them. He acts like a monster. It's disgraceful... and a little scary."
- "Yes, of course... our usual boundaries and personal walls are down and we can act more carefree and outspoken if we feel like. At least this is true for me... you can act like a goddess."
- "I have cursed out a lot of ppl [people], and when my bud comes over, we go into places like the African American room and yell "KKK ALL THE WAY" or go to the Jewish room and say "HEIL HITLER," but I haven't done that since I started going back to church and was saved by Jesus Christ. We were just joking, we weren't really racist."
- "Yes, but I'd rather not describe what I did. Instead, I'll just say that online, you can be absolutely ANYONE you want to be, which is why a lot of people do things that they would not normally do. In real life, people everywhere judge you based on your looks, actions, and who knows what else, but online, all that really matters is your attitude and personality."
- "Uh well, I tried cyber sex before and I wouldn't ever do that in real life. Sex period. I don't believe in premarital sex. I think that is a great gift you give your husband. I once told someone off because he/she was being perverted and talking nasty to me and I didn't like it."
- "Well, once I told this guy I met in a chat room all about me and, like, my phone number and stuff. I now realize that this was really stupid of me and will never do anything like it again cause although it's not likely, he could be a psycho or something."
- "I feel I can speak more freely to someone online about my problems because most of them don't go to my school or even the same state. I can ask them advice and they would probably give me the best because they aren't in favor of a certain person. I can introduce

myself and meet new people because it isn't as uncomfortable to look into their eyes and if you become really uncomfortable I can just get out of it by blocking them or getting offline."

- "I have had cyber sex... that's something I never have done and never will do until I'm married in real life."
- "I am much more bold online than in real life. I am VERY shy and I say things on the Internet that I normally wouldn't say in public."
- "I have lied for no reason. Actually, I told a guy I couldn't give him my number cause my mom doesn't want guys calling me cause it was during the school year. My mom doesn't really care who calls me I just didn't know what to say."
- "Yeah, I wouldn't flirt with people I just met in person, unlike on the Internet."
- "Flirt more easily, say things I wouldn't say in person, not bad things, just more honest things."
- "Yeah, because it's a lot easier to talk and get to 'know' someone online because you can't see their face. I never have done anything bad but I've been a lot more easy going and free for what I'd say online then in a live situation which in someways have helped me to be more comfortable talking to new guys in person."
- "Well, honestly... yes. I had cyber sex! I will never have real sex until I am married, after I engaged in cybering, I totally felt grossed out, like I know I was doing something wrong! I will not make that mistake again."

Yet, even with all of this, parents are often reluctant to read their children's online public posts. They feel that they may be invading their privacy. This can be very frustrating for me. I don't understand why a parent thinks that reading a post designed to be read by any of the 700 million people online is invading their privacy. The rule shouldn't be "Everyone, except the child's parent can read their public post!" Accessing their passwords without their permission, or spying on them is different, but reading something intended for public consumption isn't. It's our *obligation* to keep our children safe. Remember that! PLEASE!

When we asked them if they ever pretend to be someone else in cyberspace, here's what they answered (in their own words):

- "Of course I've pretended. Everyone does. You pretend to be older... or you pretend to be a guy... or you just pretend to be whoever you wanna be."
- "Yes, I just changed myself to be someone I wasn't because I wanted to get a different reaction from people. It gave me a way to see myself as who I wanted to be but by doing it I realized that that is not who I want to be and that I just want to be me."
- "Yes. If I am ever in a chatroom I always make up things about myself. This is why I say don't trust anyone because everybody else does the same thing."
- "Since nobody seems to be eager to talk to a 15 year old, I always pretended I was 18 year old female. However, that sometimes attracted bad attention from guys."
- "Yes. I pretended to be anyone from Leonardo DiCaprio to a serial killer."
- "I once pretended to be a 16 year old girl. I wanted to talk to my boyfriend to see if he would agree to meet her in person. He did and I told him who I really was and we broke up."
- "Yes, I've pretended to be so many people. It's fun and safe and because nobody knows who you really are."
- "Well we've ALL pretended to be older or have a different name or something. Who doesn't? It's part of the fun about being online... you can be whoever you want to be for a little while."
- "Yes, I pretended to be someone that I wish I could be like a popular person."
- "I haven't pretended to be someone else, but I have pretended to be a couple of years older than I am, because not many people my age are online to talk to, and if they are, they must be lying about their age, too."
- "No, I think it is wrong to lie to other people about who you are. I wouldn't want someone to do it to me so I don't do it to them."

When we asked them if they had ever been in a situation online that frightened them, here's what they said:

- "My friend agreed to meet a guy she met online when he came to our hometown, and she wanted some of us to come along to keep them company. I told my parents but luckily the guy's game got canceled. I wouldn't have gone and I would not support her decision to meet anyone in real life. She kinda felt betrayed but at least she's still alive."
- "Once I was scared because this guy kept telling me all this stuff about me, like my name, address, friends' names, etc. he said he knew where I lived and stuff, and I better watch out. It ended up being a joke from a friend of a friend, but I was still scared, and I was very angry at the friend who gave the person the info just to scare me. It wasn't funny."
- "Once I was on ICQ talking to a bunch of my friends when this guy I had been chatting with sent me a file. Unknowingly, I opened it and then I realized that the person had hacked into my system. Suddenly, my CD-ROM drive started opening and closing and annoying (but not threatening) messages started appearing on my screen. Soon after my mouse buttons switched functions. I had just finished a big assignment, so I was afraid the hacker would do something to wreck it. I shut down my computer and that was about all I did about it. One of my friends had a similar experience, only hers was scary and threatening. When she got hacked, pictures of a dead girl with her face smashed in appeared on her screen, along with threatening messages and sound clips."
- "I know this is normal in fact it doesn't bother me I just laugh. Most kids are always exposed to this stuff not just on the Internet so its no big deal in fact sometimes it makes it interesting. But one time this dude got really mad at me and he knew my parents were out of the state and he could have called one of my friends and found my address but instead he kept calling every 5 minutes...."

- "There was one time, when I got online to check my e-mail. I ended up going into my regular chatroom, and when I arrived, some guy started giving out my personal information. I don't know how he knew anything personal about me, but he was telling everyone in there about the frightening and terrible things that were done to me as a child. My best friend doesn't even know what happened to me when I was little. All I did was, denied all of what he said and logged off. I cried all week long."
- "This guy IM'd [instant messaged] me and my best friend and he knew all this information about us... and we hadn't even talked to him before. He knew who we were, where we lived and everything and he kept playing with our minds trying to tell us that we started IMing him first and so on. I told my parents about it but they didn't really care. So this went on for an hour and a half. I had friends try to get him to stop. He told us where he worked and he kept insisting that we go places with him like out to lunch or dinner and he would buy us x-mas and b-day presents even though we had never met him. He would leave them on his car at work for us to come and get, we would go get them and just smash them all over the ground... thinking he would get the point. He was convinced that him and my best friend were dating then I came along and I'm the one who stopped it all. No one could get this guy to stop. We changed our screen names plenty of times but he had already hacked into our account so he could always find us. Well he hacked into mine. Well in December we got a new computer and we both changed our screen names and he hasn't been able to find us since."
- "[A]bout a year ago I met a guy online and I told him my phone # and found out he lived about 5 minutes away from me we talked 4 about a week then he asked me out and I agreed. We met up at the mall he was totally normal 15 year old guy. He wasn't some psycho or anything but I got in a lot of trouble from my parents and I will never give out any personal information again. It's not safe and its a stupid idea. If anyone who reads this is thinking about giving out info to someone on the net PLEASE think twice about it you could get yourself into a lot of trouble."
- "I received a threatening E-mail from someone on my E-mail address. I immediately changed my password, and made sure that I didn't have information on my profile. I never E-mailed the person back, since that is what lets them know your account is active and they can find out more about you. Then, I decided to make sure about it, and stopped checking my E-mail account. I just got a new one."
- "I was in a chat room once and this person was threatening to kill themselves, and I find that scary. So I IM'd them not to do it, and I chatted with them for a while, and made them feel better about themselves, and promise not to do anything drastic. And they did promise."
- "I told these people to leave this foreign guy alone because they were making fun of him. They were calling him names and mocking everything he said. The people I got smart with told me I better watch my back because they could find out where I lived. That's why I left."

It would be interesting to ask your children to reply to the same questions. You might learn something about your children you didn't know.