

NJPSA'S Cyber Safety Toolkit: Solutions for Schools



Table of Contents

Introduction

1. Cyber Problems

- Cyber Bullying
- Cyber Predators
- Cyber Memory
- Cyber Crime
- Cyber Cheating

2. Solutions for Cyber Safety

Prevent Cyber Bullying

- Focus on the School Environment
- Garner Staff and Parent Support
- Form a Group to Coordinate Efforts
- Train Staff
- Establish and Enforce School Rules
- Increase Adult Supervision
- Intervene Consistently and Appropriately
- Focus Class Time on Prevention
- Continue Efforts Over Time

3. What the Law Requires: Legal Issues Related to Cyber Bullying

- Legal Definition of Bullying
- Conduct Away from School Grounds
- Cyber Bullying and Student Due Process Rights
- Landmark N.J. Supreme Court Decision Sets New Standard
- Case Law Regarding Student Discipline and Cyberspace
- Searches of Cell Phones and Other Hand Held Devices

4. Additional Steps for Cyber Safety

- Prevent a Crime
- Write an Acceptable Use Policy (AUP)
- Build Firewalls and Network Security
- Install Filtering Software
- Write Policies Restricting What You Can Publish Online
- Link with Law Enforcement

5. Agencies Investigating Cyber Crime

6. Talking Points to Use with School Staff

- Talking Points to Use with Families

7. Tips for Families of Middle and High School Students

- Tips for High School and Middle School Students

8. Tips for Families of Elementary Students

- Tips if Your Child Becomes a Victim of Cyber Bullying
- Cyber Safety Tips for Elementary School Students

9. Links and Resources

10. Welcome to Cyberspace: The New Vocabulary

- Top Cyber Acronyms

11. Top 15 Social Networking Sites

- Additional Social Networking Sites

NJPSA'S Cyber Safety Toolkit: Solutions for Schools



Introduction

By law, New Jersey school districts are required to have and implement policies prohibiting bullying, including cyber bullying, an event that occurs when one or more people use technology to harm, harass, intimidate, or reject another person. But cyber bullying is only one of the challenges technology and cyber space pose to school leaders. Developing and implementing effective policies regarding students' use of cell phones, the internet, email, and instant messaging are among a school leader's most challenging responsibilities. No school is unaffected. Research shows that cyber bullying now begins in elementary school, increases in middle school, and decreases in high school. This toolkit is designed to help school leaders formulate effective policies and strategies to not only prevent and respond to cyber bullying, but to keep students as safe as possible in cyber space.

Cyber Problems

1. Cyber Bullying

Cyber bullying includes: repeatedly sending offensive, rude, and insulting messages; distributing or posting derogatory information or pictures about another; impersonating someone; sending offensive messages; tricking someone into revealing embarrassing information; and sending pictures of someone being beaten up. Cyber bullying by proxy is when a cyber bully gets someone else, usually an unwitting accomplice including principals, teachers, and parents, to harass or harm the victim. The cyber bully makes it appear that the victim has done something wrong and then reports the wrongdoing to the authorities so that the victim is punished. The most common way to cyber bully is to discover a victim's internet account and send out hateful or insulting messages to their buddy list.

2. Cyber Predators

Cyber predators troll the internet and use ploys to lure children into their trust, and then harm them, either online or in person. The typical predator ploy is summed up in the acronym SITS for similar interests, trust, and secrecy. It starts with a "grooming" period when the predator pretends to have the same interests and problems as the child. Then, over the course of months, the predator wears down the child's defenses so that the child develops a sense of trust, always requiring that the child keep their communication secret. Ultimately, they make their solicitation either online or in person.

3. Cyber Memory

Students are many times more likely to victimize themselves than to be the victim of a sexual predator. A recent study found that 20 percent of teens had sent or posted a naked picture of themselves. A third had received such a picture or video by text message or email. One principal estimated that if she suddenly collected all students' cell phones, half might contain nude photos of students. When "sexting", students seem unaware that the internet never forgets, and it is a crime to email nude photos of children. A child sends a photo to a single friend, who sends it to another, and it is soon shared with half the student body or even posted on a website. It will remain in cyberspace forever, available to college admission officers, coaches, and prospective employers who now routinely look online for background material. Children, who are simultaneously the victim and offender, have been arrested on pornography charges.



4. Cyber Crime

Computer intrusion, or hacking, password trafficking, counterfeiting of currency, child pornography or exploitation, online stalking, identity theft, internet fraud, harassment, bomb threats and trafficking in explosive or incendiary devices or firearms are among the crimes technology and the internet have facilitated.

5. Cyber Cheating

Technology has given students who want to cheat many new options, including:

Text messages - Students contact an accomplice outside the exam room and receive answers quickly.

Cell phones with built-in digital cameras - Not as risky as text messages, this method is more common. Students photograph test questions with their cell phone cameras, send them to friends outside via MMS, and receive the answers in text or image format.

Tiny MP3 players- Students record notes, transfer the audio files to a tiny MP3 player, and play very quietly during the exam.

iPods- iPods are used to hide lists disguised as song titles. Because listening during a test is not usually allowed, students put an earphone up one sleeve, or wear a hood to hide the wires. iPods can also display images and videos -- useful for exams that require graphs.

Calculators - Programmable calculators can hold text, formulas, even pictures. Add-on memory allows students to store software, turning their calculator into a pocket notebook. Various calculators are allowed even when taking the PSAT, SAT I, SAT II, Math IC, and IIC, AP Chemistry exam, AP Physics exam, and AP Calculus exam.

Wireless earphones + microphones - These are tiny earphones that students place in their ears and are too small and too well hidden to be seen. Students also have a tiny microphone hidden in their sleeve or other places to whisper the questions. Students then call up when the teachers are not looking.

PocketPC- The Palm, "Q", Blackberry, and other personal digital assistants (PDAs), as well as some calculators allow information to be beamed across a distance via infrared, Bluetooth, or wireless internet access (if available in your school). Even without local wireless access, many PDAs have cell-based web browsers that can be dialed up from anywhere. Once connected, students have access to everything on the internet.

Invisible ink pens - Students use these to write information they will need on an exam. The ink is invisible to the naked eye, but magically illuminates when exposed to a black light, which is conveniently located on the opposite end of a pen.

Online essays for purchase- For a price, there are dozens of websites students can visit to order a stock essay of any length, or a unique one written upon request.

Online grade tampering-Students can change their grades by hacking into the school's computer system or hiring a hacker to do so.



Solutions for Cyber Safety

Prevent Cyber Bullying

The Olweus Bullying Prevention Program has been rigorously and independently researched. It is the best known bullying prevention program. It recognizes that, as with most cyber safety problems, the solution does not lie with 'stranger danger' fear tactics or filtering, but with prevention strategies where students and schools "own" the problem.

It advocates for, first and foremost, the warm, positive interest and involvement of adults in the culture and life of the school. Its research shows that schools are most successful in preventing bullying when they set firm limits on unacceptable behavior; consistently use non-physical, non-hostile negative consequences when rules are broken; and when all school employees and volunteers act as authorities and positive role models. Consistency in these approaches is the key to success.

The program's best practices in bullying prevention and intervention follow:

Focus on the School Environment

Experts agree that the best strategy to address cyber bullying is to prevent it from occurring in the first place. The best prevention is a school environment that nurtures respectful relationships among all members of the school community. The ideal situation exists when district and school leaders, teachers, staff, parents, students, community members, and community agencies work together toward the common goal of creating a positive and healthy school climate.

Below are the major components and tasks for creating a safe, respectful, and connected school climate:

- Assess the school's emotional climate. Anonymous surveys, face-to-face interviews, and focus groups with students, staff, parents, and community leaders have all been used to gather real-time data and the findings used to inform planned changes.
- Specifically assess bullying in the school.
- Emphasize the importance of listening in school. When staff members listen empathetically to students, especially for feelings, they gain the courage needed to break an ingrained code of silence. Listening to behavior, particularly aggressive behavior, can help identify students who do not know how to discuss or handle anger or other difficult emotions.
- Take a strong but caring stance against the code of silence. Talk with students about the harm it does, and how talking to a trusted adult can prevent pain and even tragedy. Work actively to change the perception that talking to an adult about a student doing something hurtful and wrong is considered "snitching."
- Empower students by involving them in planning, creating, and sustaining a school climate of safety and respect. Use the school climate survey to identify challenges and enlist input from students to address those challenges.



- Ensure that every student feels that he or she has a trusting relationship with at least one adult at school. One school listed every student's name on paper and distributed it to all staff. Administrators, teachers, and support staff put a star next to the name of students with whom they had a strong connection. The staff then focused on connecting with students who received the fewest stars.
- Create a number of mechanisms for developing and sustaining a healthy school climate. Mechanisms include: a committee of staff and students who discuss the school climate and how to improve it; character education programs and concept interwoven into all subjects; peer tutors; mentor programs; an annual climate survey; ongoing professional development programs for staff; and tracking outputs such as academic performance and incidents of violence.
- Be aware of the school's physical environment and its effect on creating comfort zones. A building's space, architecture, and lighting contribute to the emotional climate. Consider whether changes in lighting, the school schedule, or the assignment of teachers and students into smaller, mutually intersecting and supportive groups could help compensate for a building's limitations.
- Bring all the stakeholders to the table whenever undertaking a major change. People support most what they believe they have had genuine input in creating.
- The school climate is most influenced by people's behavior: the principal's open door policy; staff members who listen empathetically; students who have been empowered to participate in the school's culture; and local community leaders and families who connect with and contribute to the life of the school.

Garner Staff and Parent Support

Work closely with students and families to make sure they take cyber bullying as seriously as you do. All school staff can participate in discussion groups. Since cyber bullying may not actually be committed while your students are in school, it's important to involve families. At Back to School Night, parent conferences, in-service programs, etc. communicate how the school's climate and programs are working to prevent cyber bullying before it begins.

Form a Group to Coordinate Efforts

Establish a bullying prevention coordinating committee. This should include members of the larger cyber safety committee referenced above, a counselor or social worker, a coach, classroom teacher, and support staff such as a bus driver and custodian. Include members of existing related groups, if available, such as a character education group, discipline committee, a site-based leadership team, etc...



Train Staff

Begin by defining cyber bullying to make sure that everyone is on the same page. Keep the definition simple so that students can understand it too. For example, the Committee for Children, says cyber bullying is “when one or more people intentionally harm, harass, intimidate, or reject another person using technology.” Provide examples such as:

- Sending mean, embarrassing, or threatening messages to a classmate via email, IM (instant messaging), or text messages. Spreading rumors about classmates through email, IM, or text messages.
- Creating a web site or MySpace (or other social-networking) account that targets another student.
- Sharing fake or embarrassing photos or videos of classmates with others via a cell phone or the web.
- Stealing a classmate’s login and password to send mean or embarrassing messages from his or her account.

Conduct committee and staff training, including educational support personnel. Invest in conflict resolution curricular materials that provide staff and student training in solving problems and conflicts. (Many of the websites listed in the Resources section of this toolkit provide information on staff and student training.) Neither conflict resolution or mediation, however, should ever be used to address any form of bullying. Bullying must be dealt with by administrators.

Establish and Enforce School Rules

Introduce the school’s rules and policies against bullying with an all-school kick-off event. Be sure that the rules address cyber bullying. Teachers need to know they cannot tolerate name calling. Supervising and limiting students’ use of the internet and cell phones in school to certain times and places are key to combating cyber bullying. Many schools add a provision to their acceptable-use policy reserving the right to discipline a student for actions taken out of school, 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 the offending behavior a contractual, not a constitutional, issue. Each year, schools can ask students and parents or guardians to sign the acceptable user policy.

Increase Adult Supervision

Review and refine the school’s supervision of students’ use of technology thereby increasing adult supervision in high risk areas, such as gyms, playgrounds, and lunch rooms. Consider the following:

- Have adults actively engage students in board games, sports, or arts and crafts, particularly if the lunch period is longer than students need to eat.
- Create different areas on the playground for different activities. Implement clear and organized entrance and exit procedures for large numbers of students.
- Provide a system where teachers advise lunch room staff how certain students are behaving and vice versa.
- Assign adults to hallways when students are transitioning.



- Closely monitor students' use of computers.
- Ensure that an adult should be nearby when students are online.
- Develop a "buddy system" that can extend adults' eyes and ears as well as protect vulnerable students. Assign the following: caring students to newcomers or students without friends to facilitate easy transitions; older, bigger students to look out for students who seem to be bullied by others; one adult to meet frequently with the "mentors" to find out about problems that may be brewing.

In addition to increasing adult supervision, schools are legally required to set up an anonymous tip line system so students can report cyber bullying without fear. This step is vulnerable to false reports, so each report must be carefully investigated. Also, schools can install filtering and tracking software on all computers. (See the Additional Steps section of this toolkit for information on tracking software.)

Intervene Consistently and Appropriately

Investigate reports of cyber bullying immediately. If cyber bullying occurs through the school district's internet system, you are obligated legally to take action. Talk with all students about the destructive consequences of cyber bullying whether in or out of school. Cyber bullying that occurs out of school can travel like wildfire among students, and can affect how they behave and relate to each other at school. If the cyber bullying occurs out of school, schools can still take action. They may notify parents of victims, and parents of students known or suspected to be cyber bullying. Schools can notify the police if the known or suspected cyber bullying involves a threat, and may closely monitor the behavior of the affected students at school for possible bullying. Also, they may investigate to see if the victim(s) of cyber bullying could use support from a school counselor or school-based mental health professional.

School leaders should contact the police immediately if known or suspected cyber bullying appears to involve threats of violence, extortion, obscene or harassing phone calls, or text messages, harassment, stalking, hate crimes, or child pornography.

Focus Class Time on Prevention

Teachers and coaches should post and enforce the school's rules against bullying, hold regular class or team meetings about bullying, and address the subject when meeting with students' parents. The school's character-building courses and class activities that foster healthy conflict resolution methods should address cyber bullying as well.

Continue Efforts Over Time

The threats of today did not exist yesterday, and there will be new threats tomorrow. Facebook now has two million subscribers, double the number from just eight months ago. New technologies such as Twitter, or micro-blogging, and Skype, a free on-line video and audio service, grew in a flash. When students know more about emerging technologies than teachers and school leaders, they feel empowered to use them without consequences. Ongoing professional development about emerging technologies and their use in bullying is key. Consider subscribing to an internet magazine and keep copies in the teacher's room and administrative offices.



What the Law Requires

Legal Issues Related To Cyber Bullying

A common misperception exists that school officials are legally powerless to address incidents of cyber bullying. School administrators are unsure as to the difference between “kids being kids” and cyber bullying. In addition, incidents of cyber bullying often happen away from school grounds leaving school administrators to believe they either have: 1) no authority to act; or 2) enough to do addressing those incidents that happen in school, without worrying about incidents that occur outside of school. Even if administrators wish to act, it is not always easy to determine what actually occurred and who was responsible for cyber bullying, since emails, text messages, and other forms of electronic communication do not always clearly identify the message sender. Finally, school administrators are leery about violating student’s legitimate First Amendment rights. Administrators need to know that when students cross the line, their speech is not constitutionally protected.

Legal Definition of Bullying

Let’s begin our legal discussion with some basic definitions:

“Harassment, intimidation, or bullying” may include “any gesture or written, verbal or physical act, or any electronic communication, reasonably perceived as being motivated either by any actual or perceived characteristic, such as race, color, religion, ancestry, national origin, gender, sexual orientation, gender identity or expression, or a mental, physical or sensory handicap, or by any other distinguishing characteristic, that takes place on school property, at any school-sponsored function, or on a school bus and that:

- a. a reasonable person should know, under the circumstances, will have the effect of harming a student or damaging the student’s property, or placing a student in reasonable fear of harm to his person or damage to his property; or
- b. has the effect of insulting or demeaning any student or group of students in such a way as to cause substantial disruption in, or substantial interference with, the orderly operation of the school.

See N.J.S.A. 18A:37-14.

“Electronic communication” means “a communication transmitted by means of an electronic device, including, but not limited to, a telephone, cellular phone, computer, or pager.” See N.J.S.A. 18A:37-15.1.

Conduct Away From School Grounds

At first blush, this definition may appear to exclude any cyber bullying incidents that do not occur on school grounds, at a school function, or on a school bus. However, the New Jersey Department of Education’s model policy on bullying and harassment was revised in November 2008 to specifically reference cyber bullying and make clear that school districts are required to address conduct away from school grounds in certain instances. In addition, New Jersey case law specifies that school districts have a duty to address conduct away from school grounds under certain conditions. See *R.R. v. Board of Educ. of Shore Reg. High School Dist.*, 109 N.J. Super. 337 (1970); *L.W. v. Toms River School Dist.*, 189 NJ 381 (2007).



The standard for when a school district must address conduct away from school grounds is found in *N.J.A.C. 6A:16-7.6*, which provides that a school district may impose discipline for conduct away from school grounds when “it is reasonably necessary for the student’s physical or emotional safety, security and well-being, or for reasons relating to the safety, security and well-being of other students, staff or school grounds” and the conduct “materially and substantially interferes with the requirements of appropriate discipline in the operation of the school.”

This standard is critical when considering issues of cyber bullying. Some incidents of cyber bullying, such as students texting each other, may occur on grounds. However, cyber bullying often occurs away from school grounds. In addition, cyber bullying often is meant to cause emotional, rather than physical, harm to students. In these cases, a school district still has a duty to act.

Cyber Bullying and Student Due Process Rights

The school principal’s job would be far easier if he or she knew exactly what happened in an alleged cyber bullying incident. Most cases are not that simple. The cyber-bully may be using an online name that is not readily identifiable. There may be no physical evidence of the alleged bullying, since text messages or instant messages may not have been saved. The principal may be given incomplete information, such as a print out of one student’s instant message, where the other student involved perhaps sent an equally inappropriate or inflammatory message.

Unfortunately, school principals often must make decisions with less than perfect information. The United States Supreme Court has recognized this practical reality. In *Goss v. Lopez*, 419 U.S. 565 (1975), the Court held that a school district may impose a short-term student suspension (up to 10 consecutive school days) after providing basic due process rights to a student. These rights include: informing the student what he or she is accused of doing; giving the reason for the suspension; and providing the student an opportunity to tell his or her side of the story. The principal may then impose discipline, consistent with board policy. The student does not have a right to a formal hearing before the board of education prior to a short-term suspension. Nor does the principal have to wait to meet with parents prior to imposing discipline, although meeting with the parents may be a step a principal chooses to take in some cases prior to imposing discipline.

For long-term suspensions (more than 10 consecutive school days) students have greater due-process rights. These rights include all the rights afforded for short-term suspensions, plus written notice, including specific charges, to the parents within two school days of the initial suspension and the right to a formal hearing before the board of education. The formal board hearing must take place within 30 days of the initial suspension. Prior to any hearing, the parent must be provided with a list of witnesses, including corresponding statements and affidavits. At the hearing, the student may be represented by counsel who has the right to confront and cross-examine witnesses. See *N.J.A.C. 6A:16-7.3*.

Landmark N.J. Supreme Court Decision Sets New Standard

On February 21, 2007, the New Jersey Supreme Court issued a landmark ruling in the case of *L.W. v. Toms River Regional School District*, 189 N.J. 381 (2007), regarding the legal standard to be applied in determining if school districts are to be held liable for student-on-student harassment based on sexual or affectional orientation. The Supreme Court held that under the New Jersey Law Against Discrimination, school districts are to be held liable for such harassment when a school district knew or should have known of the harassment and failed to take actions reasonably calculated to end the mistreatment



and offensive conduct. *Id.* at 36. The Court held that school district liability for student-on-student harassment will no longer be limited to instances where the district was “deliberately indifferent” in responding to the harassment. *Id.* at 27. The Court recognized that school districts cannot be expected to prevent every single incident of student taunting or harassment and emphasized it was not imposing a strict liability standard. Rather, it held that a case-by-case factual analysis is required to determine if the district’s response in the particular case was reasonable under the circumstances. *Id.* at 33.

L.W. was a student in the Toms River Regional School District. Starting in the fourth grade, other students began taunting him with homosexual epithets such as “gay,” “homo,” and “fag.” The bullying intensified in regularity and severity from the fourth to seventh grade. School officials first learned of the behavior in fifth grade. During a period of less than four months while in the seventh grade, L.W. was subjected to at least nine incidents of bias-based harassment, two of which included some form of physical assault. The incidents collectively involved a total of 18 different students who participated in some form of harassment of L.W. The incidents ranged from several instances of verbal abuse and assaults, including derogatory terms such as “faggot” to instances of physical assaults to L.W.’s person including a student rubbing against L.W. in the lunch line, L.W. being struck by a play book as well as incidents occurring during and after the school day both on and off of school property.

While not deciding whether the Toms River Regional School District was civilly liable for failing to stop the harassment, the Court sent a clear message that the law has changed regarding bullying in the following ways:

- For the first time, the Court recognized a private right of action for student-on-student harassment under New Jersey’s Law Against Discrimination (LAD). This state statute includes far reaching protections against discriminatory treatment based on a wide range of characteristics, including race, gender, disability, and sexual orientation. In the past the LAD had been used in the school setting to address discriminatory treatment by a supervisor against an employee, or in cases of harassment by co-workers, where a supervisor failed to take effective action to prevent or stop the harassment, but had never previously been applied to a failure by a school district to respond to student-on-student harassment. *Id.* at 22.
- The Court rejected the “deliberate indifference” standard that had been used in prior cases where school districts were sued under the federal Title IX for failing to stop student-on-student harassment. *Id.* at 27.
- School districts are required to take effective steps to end harassment. “Effective” remedial measures are those reasonably calculated to end the harassment. The “reasonableness” of an employer’s remedy will depend on its ability to stop the harassment by the person who engaged in harassment. *Id.* at 29.
- School districts must now do more than simply rely on existing discipline policies. Districts must assess the effectiveness of existing policies. If student bullying and harassment continues, the district must show evidence that it has taken steps to revise ineffective policies and procedures. *Id.*

The Court in *L.W.* noted that determining if a district acted reasonably is a heavily fact-intensive inquiry that must consider the “totality of the circumstances.” *Id.* at 32. Factors to be considered include:

- The students’ ages, developmental, and maturity levels;
- School culture and atmosphere;
- Rareness or frequency of the conduction;
- Duration of the harassment;
- Extent and severity of the conduct;



- Whether violence was involved;
- Prior history of harassment within the school district, the school, and among individual participants;
- Effectiveness of the school's response;
- Whether the school district considered alternative responses;
- Swiftiness of the school district's reaction;
- New Jersey Department of Education (NJDOE) regulations, model policies, and other guidance; and
- In many cases, expert opinion regarding the reasonableness of the district action at the time of the incident or incidents. *Id.*

The decision in *L.W. v. Toms River* provides a far broader legal basis for holding school districts liable in future cases of student-on-student harassment, at least where such harassment is linked to protected classifications such as sexual or affectional orientation, race, ethnicity, gender, and disability. Coupled with the recent enactment of New Jersey's anti-bullying legislation, there is now a clear message that it is no longer legally sufficient for school officials to react piecemeal to individual incidents of student misconduct where that misconduct is motivated by bias. Unlike in the *L.W.* case, all New Jersey school districts now have the benefit of comprehensive guidance from the NJDOE on how to address issues of bullying, harassment, and intimidation.

Courts will expect in future cases that: 1) all school employees are thoroughly familiar with the NJDOE guidance; 2) school staff have been properly trained; and 3) the district is in fact implementing the required policies to deal with issues of harassment and discrimination. Districts must react swiftly to reports of harassment, and must ensure that information is effectively shared so that teachers and administrators are aware of any prior history of harassment.

In addition, where existing discipline policies are not effective in stopping harassment, it is critical that districts consider alternative approaches. It will not be sufficient for a district to claim that it follows an existing discipline policy, if that policy is clearly not working to stop harassment in a given case. School principals and other district administrators have a vital role to play in leading the effort to ensure that district policies are comprehensive, known by all stakeholders, and constantly being monitored and revised as needed to ensure their effectiveness.

Case Law Regarding Student Discipline and CyberSpace

A recent New Jersey case provides guidance on determining the free speech rights of students engaging in cyber-speech. The case, *Dwyer v. Oceanport School District, et.al.* Civ. 03-6005 (SRC), U.S. Dist. (N.J. Mar. 31, 2005 (Media Law), involved Ryan Dwyer, a 14-year old 8th grade student at the Maple Place School in the Oceanport School District, who created a website from his home called "I hate Maple Place." The website was made accessible to anyone. It included a "Home" page, an "About" page, a "Favorite Links" page, a "What's New" page, a "Guest Book" page, and a "Custom" page. Among other things, the home page said "down with Maple Place." It was dedicated to "showing students why their school isn't what it is cracked up to be."

The guest book page contained certain warnings. It warned guest users from using profanity and from making any threats. Nonetheless, some of the guests used profanity and still made threats. The student who created the website had no control over the messages that were posted by guest users.



The principal viewed the website and contacted the superintendent. When the superintendent heard that in addition to certain profanity, threats were also posted on the website, e.g.[the] “principal should walk into oncoming traffic,” he directed the principal to call the police.

The principal and the superintendent also met with the Ryan Dwyer and his father. They informed the Dwyers that Ryan would be disciplined and because of the threats posted, the matter had been given to the police to investigate. The discipline consisted of a five day suspension, suspension from the school baseball team for one month, and exclusion from the 8th grade class trip to Philadelphia. Ryan and his parents then filed a law suit. There were a number of issues addressed by the court.

Can a Student Be Held Responsible for Statements Made by Others on the Guest Page of the Website?

The court noted that Ryan had warned guests from posting on the website any profanity or any threats. Citing Section (c)(1) of the “Communications Decency Act,” 47 U.S.C. §230, the court concluded that a student, as the publisher of the website, could not be held accountable for what the guests to the website had posted. *Dwyer* at 9. The Communications Decency Act provides in pertinent part that “no provider or user of an interactive computer service shall be treated as the publisher or speaker of information provided by another information provider.” *Id.* The court said that in the context of this case everyone who had posted messages on the Ryan’s website was an “information content provider.” *Id.* While the school could have lawfully disciplined the student if he had posted the objectionable statements, it could not punish him for comments made by other individuals in his guest book.

Did the Website Disrupt the School?

The standard articulated by the court is whether the website and the statements that appeared on it “materially and substantially” interfered with the requirements of “appropriate discipline in the operation of the school.” *Id.* at 15. (citing *Tinker v. Des Moines Independent School*, 393 U.S. 503, 509 (1969)). This means more than discomfort and unpleasantness. As the school district was not able to point any material disruption of the school, or of any disruption of any activity in the school, the court said that it had no choice but to conclude that the website, however offensive to some, was not disruptive.

Did the Student’s Discipline Violate His First Amendment Rights?

The court concluded that it did. The website was created off school premises, on the student’s home computer, and not during school time. The student himself did not write any threatening remarks about anyone in the school. He only wrote “opinions” that included statements such as a certain teacher was the “worst” teacher in the school because she had a “short temper,” that the principal was “not a friend and was a dictator,” that a certain other teacher was the “coolest” teacher in the school, that protests were not illegal, that school was boring, that students should wear political t-shirts to “annoy” teachers, that students should make stickers that say “I hate Maple Place,” and that the principal had “flipped out” using an illustration of his head upside down. Opinion, said the court, is protected. *Id.* For Ryan’s speech to have been constitutionally proscribed the school district would have had to have demonstrated a “specific and significant fear of disruption, and not just some remote apprehension of disturbance.” *Id.* (citing *Saxe v. State College Area School District*, 240 F.3d. 200, 211 (3d Cir. 2001)).



Searches of Cell Phones and Other Hand Held Devices

One final legal issue to be considered is the legality of school officials searching cell phones, IPODs, Blackberrys, and other handheld devices. School officials often confront this issue when students bring cell phones or other hand-held devices to school and use the cell phones or devices in school, in violation of school district policies. Such impermissible uses include talking on a phone during class, texting during class, “sexting” which involves sending sexually explicit images to others, using devices to facilitate cheating on exams, and so on.

It is important to note that school officials must respect students’ Fourth Amendment Rights in searching such devices. The Fourth Amendment protection against unreasonable searches and seizures applies in public schools as well as in law enforcement, the “reasonableness” of a search is measured differently in the school context. Whether a search is reasonable involves a balance of the student’s legitimate expectations of privacy and personal security and the school’s need for effective order and discipline.

The legal parameters of such searches were outlined by the United States Supreme Court in the case of *New Jersey v. T.L.O.*, 469 U.S. 325 (1985). Determining the reasonableness of any search involves a twofold inquiry: first, one must consider “whether the... action was justified at its inception;” second, one must determine whether the search as actually conducted “was reasonably related in scope to the circumstances which justified the interference in the first place.” *Id.* at 341 citing *Terry v. Ohio*, 392 U.S. 1, 20 (1968). Under ordinary circumstances, a search of a student by a teacher or other school official will be “justified at its inception” when there are reasonable grounds for suspecting that the search will turn up evidence that the student has violated or is violating either the law or the rules of the school. *Id.* Such a search will be permissible in its scope when the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of the age and sex of the student and the nature of the infraction. *Id.*

Applying this standard to cell phones and other hand-held devices, let’s consider a few scenarios. If a student was seen talking on a cell phone during class in violation of school district policy, a teacher would be justified in seizing the phone and turning it over to the school principal. The principal could then return the cell phone either to the student or a parent at the end of the school day. The teacher would not be justified in searching the phone, since there would be no reason to believe that the search is justified at its inception. The only suspected violation in this case is the use of the phone in class, which is addressed simply by confiscating the phone.

Conversely, if a school official detects a student texting during the middle of an exam, the teacher would be justified in seizing the phone and turning it over to the school principal. The principal in turn would be justified in searching the phone since he or she would have reasonable suspicion that the student was involved in cheating. The same would be true if the principal had reason to believe the cell phone was being used to sending bullying or sexually inappropriate text messages to other students.

It is important to stress that under no circumstances should the individual teacher be searching the cell phone or other handheld devices, unless such a search is done with the specific authorization of a school administrator. In order to ensure that student searches are being done in a proper manner, school administrators need to maintain tight control of the search process.



Additional Steps for Cyber Safety

Prevent a Crime

Go to <http://www.ic3.gov/preventiontips.aspx#item-13> for tips about how school staff and students can avoid being victims of a wide array of internet crimes such as the Nigerian letter, phishing and spoofing — all schemes to defraud money from people on line.

Write an Acceptable Use Policy (AUP)

An AUP is a statement that is read and signed by every student, parent/guardian, and district representative. It should describe in detail, using specific examples, how, when and where students and staff may and may not use school computers and internet access. It should include guidelines, penalties, a disclaimer releasing the school from certain liabilities, and a provision that allows administrators and teachers to monitor network transmissions, including e-mail.

Build Firewalls and Network Security

Network security administrators in schools can install software programs that monitor the information that is transmitted to and from the school servers (computers that act as the central “gateway” to the internet and often the connector of computers on the local area network or LAN). This is commonly known as a firewall, as it prevents certain types of information, files, and programs from crossing into or out of the school’s computer environment. This is a preventive form of network security. Firewalls are often used to prohibit teachers or students from downloading free software, submitting certain information online, or opening e-mail attachments. Downloads and email attachments can deliver viruses that can debilitate computer systems. They can also compromise the security of a school network, leaving students’ and teachers’ personal information like grades, names, addresses, and other private information open to hackers and other illegal entities.

Install Filtering Software

Many schools use filtering software to keep students from seeing inappropriate material. This software restricts access to certain sites, based on keywords or phrases that are deemed unacceptable. This offers protection from some sites. However, the owners of these sites are now wise to blocking efforts and sometimes create innocuous sounding URLs that in fact promote material that is not appropriate for the school setting. There are limitations to the effectiveness of filters. They may keep students from visiting legitimate sites that contain sensitive keywords. If students in a health class are researching cancer, they may be unable to view pages relating to breast cancer because of the filtering of the word “breast.” Some filters prohibit the use of chat or even message boards and blogs due to inappropriate content and safety risks for students. Unfortunately, this also makes class participation in legitimate educational interactive sites virtually impossible.



Write Policies Restricting What You Can Publish Online

Internet safety goes beyond the scope of what can be accessed online. It also concerns what schools can post or publish on a website. Districts should have formal policies about restrictions. For example, school web pages are certainly affected by security concerns. Some schools restrict the use of student photos on their pages. Others use photos, but no names. Still others may allow photos with first names only, but require parental permission.

Link with Law Enforcement: How to Investigate and Handle Suspected or Reported Problems/Dangers/Threats

As you can see on the chart below, different federal agencies respond to different cyber crimes. However, schools should report suspected crimes to their local police. Schools' districts should have a policy identifying who places that call. The local police will then alert the appropriate agency.

The Internet Crime Complaint Center (IC3) is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C). IC3's mission is to serve as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime. The IC3 gives the victims of cyber crime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations. For law enforcement and regulatory agencies at the federal, state, and local level, IC3 provides a central referral mechanism for complaints involving Internet related crimes.

One of the main resources for law enforcement is a network of law enforcement officers known as Cyber Law Enforcement. These officers specialize in cyber crime investigation and training. The issues they investigate include child pornography, cyber stalking, cyber scams and fraud online. Their website is located at www.cyberlawenforcement.org.



Agencies Investigating Cyber Crime

New Jersey Attorney General
25 Market St.
Trenton, NJ 08611
(609) 292-4925

Appropriate Federal Investigative Law Enforcement Agencies

Computer intrusion (i.e. hacking)

- FBI local office
- U.S. Secret Service
- Internet Crime Complaint Center

Password trafficking

- FBI local office
- U.S. Secret Service
- Internet Crime Complaint Center

Counterfeiting of currency

- U.S. Secret Service

Child pornography or exploitation

- FBI local office
- If imported, U.S. Immigration and Customs Enforcement
- Internet Crime Complaint Center

Child exploitation and internet fraud matters that have a mail nexus

- U.S. Postal Inspection Service
- Internet Crime Complaint Center

Internet fraud and SPAM

- FBI local office
- U.S. Secret Service (Financial Crimes Division)
- Federal Trade Commission (online complaint)
- If securities fraud or investment-related SPAM e-mails, Securities and Exchange Commission (online complaint)
- The Internet Crime Complaint Center

Internet harassment

- FBI local office

Internet bomb threats

- FBI local office
- ATF local office

Trafficking in explosive or incendiary devices or firearms over the internet

- FBI local office
- ATF local office



Talking Points to Use with School Staff

When school employees use the internet inappropriately, it can cause scandal and heartache. Include a discussion about the use of technology and internet in your orientation session for new employees, your Back to School Welcome presentation, and at staff meetings. Some school administrators also Google staff members' names to be certain that they find any unacceptable material before a parent or reporter does. Consider the talking points below regarding the staff's personal and professional use of technology:

- Tragically, educators have encountered serious problems with even the most innocent use of technology. Be careful if you are using social networking sites like MySpace or Facebook if you have a blog, or communicate with students via text messaging. It is helpful to post homework assignments and class announcements, but other activities can make you vulnerable to questions about your relationship with students. Educators have learned that information on their web pages and blog entries can result in the need for them to resign, be fired, or be reprimanded. Cell phones with photo and video capabilities have secretly recorded inappropriate videos of educators that end up on YouTube.
- Nothing you do online is confidential. There is always a way a find it.
- Do not give your cell phone number to students or use your cell phone to call students or their families, except in an extreme emergency. Students have sent obscene photos of themselves to teachers and school staff, and then reported the teacher to the police for requesting the photo.
- If you use an online program for grading or homework, please make sure your password is not guessable. Use a combination of numbers and letters and make sure it is case sensitive. Never share your password, and change it frequently.
- To determine if someone has posed as you online or posted slanderous information, Google yourself. Go to any online search engine and type in your name. We encourage you to monitor your online identity the way you do your credit report.
- If you should find a phony web profile of yourself, notify the site administrator immediately. MySpace has a specific link for educators to report fraudulent profiles.
- Think about closing your online profile. However, if you feel deleting your web page is unnecessary, consider making the following changes:
 - Do not list students as your "friends." This blurs the line between teacher and student. Remember, comments left on your page reflect on you. You may also be judged by information listed on your "friends" pages.
 - Scrutinize every photo, blog entry, and comment on your page. Consider whether to have your photo on your site. Students have found, altered, and distributed teachers' photos without their knowledge or consent. They have pasted a teacher's head shot, for example, on to a nude body, posted it online and then alerted families and friends.
 - Comments left on your site by friends and students are usually the most troublesome. Screen all comments before posting them to your page.
 - Review and edit before you post. The internet provides a sense of freedom that can lead one to share opinions freely. Share only information you are comfortable about everyone knowing — including administrators, colleagues, students, and their parents. Even typos, grammatical errors, and misspellings can cause parents and community residents to have concerns.



- Assume nothing online is ever confidential. You are still vulnerable to hacking and unwanted people accessing your page even when it is listed as private.
- Be sure to lock your workstation when you are away from your computer for even a few minutes. This will keep someone from using your computer to cause damage or conduct illegal transactions.
- I appreciate your efforts to carry out our school's internet safety and anti-bullying efforts. They are essential. Give examples: (Mr. Jones' students did a unit on internet safety. His students did the research and saw for themselves how easy it was to deceive people online. They were able to learn for themselves how many students, everyday, are preyed upon on the internet.)
- No matter what you teach, please help make our students aware of internet crime, proper internet use and computer safety. (Distribute downloadable "Tips" fliers, LINK if appropriate.)
- As a reminder, it is our district's policy never to disclose student information (or to disclose it under these conditions). The Children's Online Privacy Protection Act (COPPA), enforced by the Federal Trade Commission, requires commercial website operators to get parental consent before collecting any personal information from kids under 13 years of age. COPPA allows teachers to act on behalf of a parent during school activities online, but does not require you to do so.
- And of course, technology has made plagiarism a lot easier, but it has also made it easier to prevent and catch it. You can get extensive information about how to prevent and detect plagiarism at www.plagiarism.org.

Talking Points to Use with Families

- Most students avoid telling any adults about a cyber bullying incident because they fear adults will only make things worse. They also fear being blamed.
- Be supportive if your child is a victim of cyber bullying. Cyber attacks can wound a child in a more serious way than "name calling."
- Let your child's teacher or counselor know as soon as possible if your child has been a victim so the teacher, guidance counselor, and school team can keep an eye out for in-school bullying and for how your child is coping. You may want to notify your pediatrician, family counselor, or clergy for support.
- There are two things you must consider if you should learn of an attack. Is your child at risk of physical harm or assault? How are they handling the attacks emotionally?
- If there is any indication that personal contact information has been posted online, or your child has been threatened, you should immediately report it to your local police, not the FBI. First "save" the communication. Then take a printout of all instances of cyber bullying to show them. However, a printout is not sufficient to prove a case of cyber harassment or cyber bullying. You'll need electronic evidence and live data.



- Let the police know, if they don't seem already aware, that anti-harassment volunteers at WiredSafety.org will work with them without charge to help them find the cyber bully offline and to evaluate the case. It is crucial that all electronic evidence is preserved to allow the person to be traced and to take whatever action needs to be taken. The electronic evidence is at risk of being deleted by the internet service providers unless you notify them that you need those records preserved. The police or volunteers at WiredSafety.org can advise you how to do that quickly.
- You can install a monitoring product, like Spectorsoft, on your home computers. It collects all electronic data necessary to report, investigate, and prosecute a cyber case. 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.
- At school, we've also set up an anonymous method of reporting cyber bullying. Explain your school's method. When we receive an anonymous tip we investigate and take action quickly, and when necessary, shut down the site, profile, or stop the cyber bullying itself. Of course we're aware of cyber bullying by proxy and realize that the "victim" may be the offender and vice versa. Identify and explain your school's services and procedures when cyber bullying is confirmed.
- If you suspect your child may be the victim of cyber crime, such as computer intrusion, or hacking, child pornography or exploitation, internet fraud, SPAM, internet harassment, internet bomb threats, or trafficking in explosive or incendiary devices or firearms over the internet, report it to your local police. Each of these crimes is handled by different state and federal agencies and the police will know whom to alert. Please let your child's teacher know so she or he can be alert to your child's needs.
- Martin Luther King, Jr. once said that in the end we will remember not the words of our enemies, but the silence of our friends. We want to teach our children not to stand silently by while others are being tormented. At school we talk to students about why it is wrong to forward a hurtful email, visit a cyber bullying "vote for the fat girl" site, or allow others to take videos or cell phone pictures of personal moments or compromising poses of others. Our students benefit when families reinforce that message at home.



Tips for Families of Middle and High School Students

- Talk regularly with your teen about online activities in which he or she is involved.
- Talk specifically about cyber bullying and encourage them to tell you immediately if they are the victim of cyber bullying, cyber stalking, or other illegal or troublesome online behavior.
- Encourage your teen to tell you if he or she is aware of others who may be the victims of such behavior.
- Explain that cyber bullying is harmful, unacceptable behavior. Outline your expectations for responsible online behavior and make it clear that there will be negative consequences, such as the loss of cell phone or internet privileges, for inappropriate behavior.
- Although adults must respect the privacy of teenagers, concerns for their safety may sometimes override these privacy concerns. Tell your teen in advance that you may review his or her online communications and even their cell phones if you think there is reason for concern. That serves as a disincentive and, if it is necessary, you have not broken an unspoken trust.
- Remind teens to “Take 5!” before responding to something they encounter online. Encourage them to talk with you about the incident.
- Consider installing parental control filtering software and/or tracking programs such as WebWatcher, SpectorPro, or Spy Agent, but don’t rely solely on these tools.
- Remind teens that information such as their full name, social security number, street address, phone number, and family financial information — like bank or credit card account numbers — is absolutely private. Revealing it puts the entire family at risk.
- Talk with teens about their screen name. Remind them not to choose one that gives away too much personal information. Encourage them to think about the impression that screen names could make.
- Use privacy settings to restrict who can access and post on your teen’s website. Some social networking sites have strong privacy settings. Show your teen how to use these settings to limit who can view their online profile, and explain to them why this is important. Setting privacy limits vary from site to site, so visit the sites your child visits to learn the process before talking with your child.
- Encourage your teen to think about the language they use in a blog. The internet never forgets. One day a college admissions officer, prospective coach, or employer may see everything your teen posts on line.
- Know how your teen is getting online. Increasingly, teens are accessing the internet through their cell phones. Find out about what limits you can place on their cell phone. Some cellular companies have plans that limit downloads, internet access, and texting; other plans allow them to use those features only at certain times of day.
- Talk to your teens about avoiding sex talk online. Recent research shows that teens who don’t talk about sex with others online are less likely to come in contact with a predator.
- If you’re concerned that your teen is engaging in risky online behavior, you can search the blog sites they visit to see what information they’re posting. Try searching by their name, nickname, school, hobbies, grade, or area where you live.
- Remind your teen that most sites have links where users can immediately report abusive, suspicious, or inappropriate online behavior.



Tips for High School and Middle School Students

- Never post, email, text, or electronically communicate an indecent picture of yourself in any way. You will be breaking the law and may be prosecuted. Many children have been, including a student in North Jersey in March. She thought only her boyfriend would see her picture.
- Consider not posting your photo at all. It can be easily altered and broadcast in offensive ways. If you do post one, ask yourself whether it's one your mom would proudly display in the living room.
- Think about how different social networking sites work before deciding to join one. Some sites will allow only a defined community of users to access posted content; others allow anyone and everyone to view postings.
- Keep strict control over the information you post. We recommend that you restrict access to your page to a select group of people (for example: your friends from school, your club, your team, your community groups, and your family).
- Keep your information to yourself. Don't post your full name, Social Security number, address, phone number, or bank and credit card account numbers. Don't post other people's information, either. Be cautious about posting information that could be used to identify you or locate you offline. This could include the name of your school, sports team, clubs, and where you work or hang out.
- Make sure your screen name doesn't say too much about you. Don't use your name, your age, or your hometown. Even if you think your screen name makes you anonymous, it is easy to combine clues to figure out who you are and where you can be found.
- Post only information that you are comfortable with others seeing — and knowing — about you. Many people can see your page, including your parents, your teachers, the police, the college you apply to, or a future employer deciding whether or not to hire you.
- Remember that once you post information online, you can never take it back. Even if you delete the information from a site, older versions exist on other people's computers and will live on the internet forever.
- Flirting with strangers online could have serious consequences. Some people lie about who they are, so you may never know who you're dealing with.
- Be wary if a new online friend wants to meet you in person. Before you decide to meet someone, do your research. Ask whether any of your friends know the person, and see what background you can dig up through online search engines. If you decide to meet them, be smart about it. Meet in a public place, during the day, with friends you trust. Tell an adult or a responsible sibling where you're going and when you expect to be back.
- Trust your gut if you have suspicions. If you feel threatened by someone or uncomfortable because of something online, tell an adult you trust and report it to the police and the social networking site. You could end up preventing someone else from becoming a victim.



Tips for Families of Elementary Students

- Keep the computer in an open area like the kitchen or family room, so you can keep an eye on what your children are doing online.
- Use the internet with them to help develop safe surfing habits.
- Consider taking advantage of parental control features on some operating systems that let you manage your children's computer use, including what sites they can visit, whether they can download items, or what time of day they can be online. These features are described in your computer's manual.
- Go where your kids go online. Sign up for – and use – the social networking spaces that your kids visit. Let them know that you're there, and help teach them how to act as they socialize online.
- Review your child's "friends list." You may want to limit your child's online "friends" to a specific number of people that your child is a true, personal friend with in real life.
- Understand sites' privacy policies. Sites should spell out your rights as a parent to review and delete your child's profile if your child is younger than 13.

Tips if Your Child Becomes a Victim of Cyber Bullying

Cyber bullying can range from rude comments to lies, impersonations, and threats, so parents' responses may depend on the nature and severity of the cyber bullying. Here are some actions that you may want to take after the fact:

- Strongly encourage your child not to respond to the cyber bullying.
- Do not erase the messages or pictures. Save these as evidence.
- Try to identify the individual doing the cyber bullying. Even if the cyber bully is anonymous (e.g., is using a fake name or someone else's identity) there may be a way to track them through your internet service provider. If you suspect the cyber bullying is criminal, contact the police immediately and ask them to do the tracking.
- Sending inappropriate language may violate the "terms and conditions" of email services, internet service providers, websites, and cell phone companies. Consider contacting these providers and filing a complaint.
- If the cyber bullying is coming through email or a cell phone, it may be possible to block future contact from the cyber bully.
- Contact your child's teacher. If the cyber bullying is occurring through your school district's internet system, school administrators will intervene and do everything possible to stop it. Even if the cyber bullying is occurring out of school, make your child's teacher aware of the problem. Teachers will watch for face-to-face bullying.
- Consider contacting the cyber bully's parents. These parents may be very concerned to learn that their child has been cyber bullying others, and they may effectively put a stop to the bullying. But proceed cautiously — the person you have identified as the bully may turn out to be the victim of cyber bullying by proxy. Someone else may have hacked into their computer and "framed" them. Even if you have the correct person, the parents may react badly to your contacting them. If you decide to contact parents, communicate with them in writing, not face-to-face. Have proof of the cyber bullying (e.g., copies of emails) and ask them to make sure the cyber bullying stops.



- Consider contacting an attorney in cases of serious cyber bullying. In some circumstances, civil law permits victims to sue a bully or his or her parents in order to recover damages.
- Contact your police and your school SRO if you suspect that the cyber bullying involves acts such as:
 - Threats of violence
 - Extortion
 - Obscene or harassing phone calls or text messages
 - Harassment, stalking, or hate crimes
 - Child pornography.

Cyber Safety Tips for Elementary School Students

- When you travel into cyberspace, take your parents along. Let them know what sites you want to visit.
- Never give out personal information anywhere online, including online pen pals.
- Never send a picture of yourself to someone in cyberspace without your parent's permission.
- Websites must get your parent's permission, or your teacher's if you are in school, before they can collect personal information from you.
- Don't share your screen name, user ID, or password with anyone other than your parents. Even if someone else says that it's okay. Do not open, reply to emails, or download files that are from strangers or have strange titles in the subject box.
- Sometimes people pretend to be someone who they aren't. Be careful! It's a good idea to stick to monitored chat rooms designed just for kids.
- Never meet someone or have someone come to meet you without your parents being there. Tell your parents and leave a site if you chat with someone making you feel uncomfortable or if a site makes you upset or afraid.
- Post only information that is OK for your parents and teachers to see. They eventually will be able to see it anyway.
- Remember that once you post information online, you can never take it back. Even if you delete the information from a site, it is still on other people's computers and will live on the internet forever.



Links and Resources

CyberSmart!

The CyberSmart! Cyber Bullying Package is a positive and empowering suite of K-12 lessons provided free to schools in partnership with the National School Boards Association's Technology Leadership Network, the Character Education Partnership, the National Association of School Psychologists, and the National Cyber Security Alliance. The lessons adopt an integrated approach, based on current research findings and best practices from the fields of cyber security, school violence prevention, and character education to impact behavioral change. The resulting package of materials focuses on developing critical thinking and decision-making skills, guiding students to define the problems and issues themselves and "own" them. The package includes standards-based, non-sequential lessons designed to be integrated into the existing curriculum by classroom teachers as compared to scheduled one-time assembly programs. It also includes home connection materials and prevention activities that extend classroom learning out to the school, families, and the community. An extra bonus is optional Web 2.0 activities so that students use the web resources to spread the positive, empowering prevention message. The CyberSmart! Cyber Bullying Package can be accessed at: www.cybersmartcurriculum.org/cyberbullying/

For more information and a detailed run-through contact:

Mala Bawer, Executive Director
CyberSmart! Education
mala@cybersmart.org
Tel. 908-221-1516

To learn more about staying safe online, visit the following organizations:

Federal Trade Commission

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or receive free information on consumer issues, visit ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

The FTC manages www.OnGuardOnline.gov, which provides practical tips from the federal government and the technology industry about safe social networking.

GetNetWise - www.getnetwise.org

GetNetWise is a public service sponsored by internet industry corporations and public interest organizations to help ensure that internet users have safe, constructive, and educational or entertaining online experiences. The GetNetWise coalition wants internet users to be just "one click away" from the resources they need to make informed decisions about their and their family's use of the internet.



Internet Keep Safe Coalition - www.iKeepSafe.org

iKeepSafe.org, home of Faux Paw the Techno Cat, is a coalition of 49 governors/first spouses, law enforcement, the American Medical Association, the American Academy of Pediatrics, and other Associations dedicated to helping parents, educators, and caregivers by providing tools and guidelines to teach children the safe and healthy use of technology. The organization's vision is to see generations of children worldwide grow up safely using technology and the internet.

i-SAFE - www.i-safe.org

Founded in 1998 and endorsed by the U.S. Congress, i-SAFE is a non-profit foundation dedicated to protecting the online experiences of youth everywhere. i-SAFE incorporates classroom curriculum with dynamic community outreach to empower students, teachers, parents, law enforcement, and concerned adults to make the internet a safer place. Join them today in the fight to safeguard children's online experience.

National Center for Missing and Exploited Children - www.missingkids.com; www.netSMARTZ.org.

NCMEC is a private, non-profit organization that helps prevent child abduction and sexual exploitation; helps find missing children; and assists victims of child abduction and sexual exploitation, their families, and the professionals who serve them.

National Crime Prevention Council - www.ncpc.org; www.mcgruff.org

The National Crime Prevention Council (NCPC) is a private, nonprofit organization whose primary mission is to enable people to create safer and more caring communities by addressing the causes of crime and violence and reducing the opportunities for crime to occur. Among many crime prevention issues, NCPC addresses internet safety with kids and parents through www.mcgruff.org and public service advertising under the National Citizens' Crime Prevention Campaign — symbolized by McGruff the Crime Dog® and his "Take A Bite Out Of Crime®."

National Cyber Security Alliance - www.staysafeonline.org

NCSA is a non-profit organization that provides tools and resources to empower home users, small businesses, schools, colleges, and universities to stay safe online. A public-private partnership, NCSA members include the Department of Homeland Security, the Federal Trade Commission, and many private sector corporations and organizations.

Staysafe - www.staysafe.org

Staysafe.org is an educational site intended to help consumers understand both the positive aspects of the internet and how to manage a variety of safety and security issues that exist online.

Wired Safety - www.wiredsafety.org

WiredSafety.org is an internet safety and help group. Comprised of unpaid volunteers around the world, WiredSafety.org provides education, assistance, and awareness on all aspects of cybercrime and abuse, privacy, security, and responsible technology use. It is also the parent group of Teenangels.org, FBI-trained teens and preteens who promote internet safety.

National Cyber Security Alliance - www.staysafe.org/educators/default.html.

This site helps educators manage a variety of safety and security issues that exist online.



Cyber-Bullying Web sites

Cyber Bullying - www.kidscape.org.uk/childrenteens/cyberbullying.shtml

Cyber Bullying - www.cyberbullying.ca/info.html

What is Cyber Bullying? - www.netalert.net.au/01569-What-is-Cyber-Bullying.asp

MindOH! Foundation - www.mindohfoundation.org/bullying.htm

Cyberbullying: Cyberbullying On The Internet - www.bullyonline.org

Challenging Cyber Bullying - www.bewebaware.ca/english/CyberBullying.aspx

Internet Super Hero - Cyberbullying, Flaming, Cyberstalking - <http://internetsuperheroes.org/cyberbullying>

Cyber Snitch Headquarters (Law Enforcement) - www.cybersnitch.net

Bullying Online - www.besafeonline.org

The Positive Learning Climates Knowledge Base - www.helpforschools.com

Dealing with Online Bullies - http://cybersmartcurriculum.org/lesson_plans/68_04.Asp.

Mobilizing Educators, Parents, Students, and Others to Combat Online bullying - www.cyberbully.org

CyberTipLine

Used for reporting the exploitation of children online. In addition, extensive resources are available at:

www.cyberbully.org

www.stopcyberbullying.org

www.njbullying.org

www.easingtheteasing.com

www.njglsen.org

Books

Allan L. Beane, Ph.D., *The Bully Free Classroom*

Stan Davis, *Schools Where Everyone Belongs*

Judy S. Freedman, MSW, LCSW, *Easing the Teasing*

James Garbarino, Ph.D. and Ellen de Lara, Ph.D., *And Words Can Hurt Forever: How to Protect Adolescents from Bullying, Harassment and Emotional Violence*

New Jersey State Bar Foundation Educational Publications, *Bullying and Teasing Training for School Staff and Administrators*. To order free publications, visit the Bar Foundation online at www.njsbf.org or call 1-800 FREE LAW.



Welcome to Cyberspace: The New Vocabulary

Top Cyber Acronyms

- 1174 - Nude club
- 1337 - Elite
- 143 - I love you
- 182 - I hate you
- 2moro - Tomorrow
- 2nite - Tonight
- 2nite - Tonight
- 420 - Marijuana
- 459 - I love you
- 8 - Oral sex
- ADR - Address
- AEAP - As Early As Possible
- ALAP - As Late As Possible
- ASL - Age/Sex/Location
- AWGTHGTGTTA - Are We Going To Have To Go Through This Again
- B4N - Bye For Now
- B4YKI - Before You Know It
- Banana - Penis
- BCNU - Be Seeing You
- BFF - Best Friends Forever
- BRB - Be Right Back
- BRB - Be Right Back
- BRT - Be Right There
- BTW - By The Way
- CD9 - Code 9 - it means parents are around
- C-P - Sleepy
- CWYL - Chat With You Later
- CYA - Cover Your Ass -or- See Ya
- CYT - See You Tomorrow
- DBEYR - Don't Believe Everything You Read
- DILLIGAS - Do I Look Like I Give A Sh**
- E123 - Easy as One, Two, Three
- EM - Excuse Me
- EOD - End Of Day
- F2F - Face-to-Face
- FOAF - Friend Of A Friend
- FUD - Fear, Uncertainty, and Disinformation
- FWIW - For What It's Worth
- GR8 - Great
- HAK - Hugs And Kisses
- ILU - I Love You
- ILY - I Love You
- IMHO - In My Humble Opinion
- IMNSHO - In My Not So Humble Opinion
- IRL - In Real Life
- ISO - In Search Of
- J/C - Just Checking
- J/K - Just Kidding
- KFY -or- K4Y - Kiss For You
- Kitty - Vagina
- KOTL - Kiss On The Lips
- KPC - Keeping Parents Clueless
- L8R - Later
- L8R - Later
- LD - Long Distance -or- Later Dude
- LMAO - Laughing My Ass Off
- LMIRL - Let's Meet In Real Life
- LMK - Let Me Know
- LOL - Laughing Out Loud -or- Lots of Love
- LOL - Laughing Out Loud -or- Lots of Love
- LYLAS - Love You Like A Sister



- MHOTY - My Hat's Off To You
- MOOS - Member Of The Opposite Sex
- MorF - Male or Female
- MOS - Mom Over Shoulder
- MOSS - Member(s) Of The Same Sex
- NALOPKT - Not A Lot Of People Know That
- N-A-Y-L - In A While
- NAZ - Name, Address, Zip (also means Nasdaq)
- NIFOC - Nude In Front Of The Computer
- NIMBY - Not In My Back Yard
- NM - Never Mind -or- Nothing Much -or- Nice Move
- NMU - Not Much, You?
- NP - No Problem -or- Nosy Parents
- NUB - New person to a site or game
- OIC - Oh, I See
- OLL - OnLine Love
- OMG - Oh My God
- OSIF - Oh Sh** I Forgot
- OT - Off Topic
- OTP - On The Phone
- P911 - Parent Alert
- PAL - Parents Are Listening
- PAW - Parents Are Watching
- PIR - Parent In Room
- POS - Parent Over Shoulder -or- Piece Of Sh**
- POV - Point Of View
- PRON - Porn
- QT - Cutie
- RBTL - Read Between The Lines
- RN - Right Now
- ROTFL - Rolling On The Floor Laughing
- ROTFLMAO - Rolling On The Floor Laughing My Ass Off
- RT - Real Time
- RTM - Read The Manual
- RU - Are You?
- RU/18 - Are You Over 18?
- RUH - Are You Horny?
- RUMORF - Are You Male OR Female?
- S2R - Send To Receive
- SH - Sh** Happens
- SITD - Still In The Dark
- SITD - Still In The Dark
- SMEM - Send Me E-Mail
- SMIM - Send Me an Instant Message
- SO - Significant Other (spouse, boy/girlfriend)
- SOHF - Sense Of Humor Failure
- SOL - Sh** Out of Luck
- SorG - Straight or Gay
- STBY - Sucks To Be You
- SWAK - Sealed (or Sent) With A Kiss
- SWDYT - So What Do You Think
- TDTM - Talk Dirty To Me
- TFH - Thread From Hell
- THX or TX or THKS - Thanks
- TLC - Tender Loving Care
- TMI - Too Much Information
- TMM - Too Many Minutes
- TOM - Tomorrow
- TS - Tough Sh** -or- Totally Stinks
- TTFN - Ta Ta For Now
- TTYL - Talk To You Later -or- Type To You Later
- TYVM - Thank You Very Much
- UR - You Are
- VBG - Very Big Grin
- WEG - Wicked Evil Grin
- WFM - Works For Me
- WTF - What The F***



- WTH - What The Heck
- WUF - Where You From
- WYCM - Will You Call Me?
- WYRN - What's Your Real Name?
- WYWH - Wish You Were Here
- XOXO - Hugs and Kisses

Sexually Explicit

- RTFM - Read The F***ing Manual
- Q2C - Quick To Cum
- FB - F*** Buddy
- MPFB - My Personal F*** Buddy
- FMLTWIA - F*** Me Like The Whore I Am
- IF/IB - In the Front -or- In the Back
- IIT - Is It Tight?
- J/O - Jerking Off
- DUM - Do You Masturbate?
- DUSL - Do You Scream Loud?
- FOL - Fond of Leather
- GNOC - Get Naked On Cam
- GYPO - Get Your Pants Off
- IAYM - I Am Your Master
- ILF/MD - I Love Female/Male Dominance
- IMEZRU - I Am Easy, Are You?
- IWSN - I Want Sex Now



Top 15 Social Networking Sites

Facebook.com: 200 million members. Was initially intended for college students. It branched out and now allows everyone membership.

MySpace.com: 200+ million members. This site is massive, boasting the largest membership of any social networking site on the Internet.

Linkedin.com: 15 million members. A powerful tool for business networking.

Friendster.com: 29 million members. Friendster was considered the top online social networking service until around April 2004, when it was overtaken by MySpace. Demographic studies indicate users are from 17 to 30 years old.

Stumbleupon.com: Boasting 2.75 million users, StumbleUpon is a web browser plug-in that allows its users to discover and rate web pages, photos, videos, and news articles. A great way to get website promotion. Bought by eBay for \$75 million in May 2007.

Del.icio.us: The website del.icio.us (pronounced as “delicious”) is a social bookmarking web service for storing, sharing, and discovering web bookmarks. The site was founded by Joshua Schachter in late 2003, and is now part of Yahoo!

Digg.com: Digg is a website made for people to discover and share content from anywhere on the internet, by submitting links and stories, and voting and commenting on submitted links and stories, in a social and democratic spirit.

Orkut.com: Orkut is an internet social networking service run by Google and named after its creator, Google employee Orkut Büyükkökten. It claims to be designed to help users meet new friends and maintain existing relationships. Now has a membership of 57 million.

Twitter.com: A free social networking service that allows users to send “updates” (text-based posts that are up to 140 characters long) via SMS, instant messaging, email, the Twitter website, or an application such as Twittrific. The site has become very popular in only a few months — a lot of people are watching it.

Classmates.com: 40 million members. One of the oldest social networking sites around, Classmates was kicked off in 1995, and has proven to be a great way for members to connect with old friends and acquaintances from throughout their lives.

Meetup.com: 2 million members. Meetup.com is an online social networking portal that facilitates offline group meetings in various localities around the world. Meetup allows members to find and join groups unified by a common interest, such as politics, books, games, movies, health, pets, careers, or hobbies.

Yahoo! 360° (a.k.a Yahoo! Days) is a personal communication portal similar to orkut and MySpace. It is currently in the beta-testing phase. It integrates features of social networking, blogging, and photo sharing sites.

Xanga.com: 40 million members. Xanga is a free web-based service that hosts weblogs, photoblogs, videoblogs, audioblogs, and social networking profiles.

Care2.com: 7.2 million members. Care2 is a social networking website that was founded to help connect activists from around the world.

Ryze.com: .25 million members. Ryze.com is a free social networking website designed to link business professionals.



Additional social networking sites include:

Bebo, BlackPlanet, aSmallWorld, Blue Dot, Bolt, Broadcaster, Buzznet, CarDomain, Consumating, Couchsurfing, Cyworld, Dandelife, DeadJournal, DontStayIn, Doostang, Ecademy, eSPIN, Faceparty, Flickr, Flirtomatic, Fotki, Friends Reunited, Gaia Online, Geni.com, GoPets, Graduates, Grono.net, Hyves, imeem, Infield Parking, IRC-Galleria, iWiW, Joga, Bonito, Last.fm, LibraryThing, LiveJournal, LunarStorm, MEETin, MiGente, Mixi, MOG, Multiply, My Opera Community, myYearbook, Netlog, Nexopia, OUTeverywhere, Passado, Piczo, Playahead, ProfileHeaven, Pownce, RateItAll, Reunion, Searchles, Sconex, Shelfari, Soundpedia, Sportsvite, Studivz, TagWorld, TakingITGlobal, The Doll Palace, The Student Center, Threadless, TravBuddy, Travellerspoint, Tribe.net, Vampire Freaks, Vox, WAYN, WebBiographies, Windows Live Spaces, Woophy, XING, Xuqa, Yelp, Zaadz, Zoomr

[Click here](#) for a more complete description of these and many other sites.

Name	Description/Focus	Registered users	Registration	Global Alexa Page ranking
Adult Friend Finder	Adults Only Dating/Hookup Network	33,000,000	Open	
Advogato	Free and open source software developers	13,575	Open	118,513
affluence	Ultra wealthy and social elite	25,000	Open, activation upon verification	36,719
Amie Street	Music		Open	29,808
ANobii	Books		Open	14,345
aSmallWorld	European jet set and social elite	270,000	Invite-only	9,306
Athlinks	Running, Swimming, Cycling, Mountain Biking, Triathlon, and Adventure Racing	54,270	Open	94,171
Avatars United	Online games and a lot of sex.		Open	
Badoo	General, Popular in Europe	13,000,000	Open to people 18 and older	213
Bahu	General, Popular in France, Belgium, and Europe	1,000,000	Open to people 13 and older	2,946
Bebo	General	40,000,000	Open to people 13 and older	108
Biip	Norwegian Community		Requires Norwegian phone number	
BlackPlanet	African-Americans	20,000,000	Open	901
Broadcaster	Video sharing and webcam chat	322,715	Open	
Buzznet	Music and pop-culture	10,000,000	Open	498
CafeMom	Mothers	1,250,000	Open to moms and moms-to-be	3,090



Name	Description/Focus	Registered users	Registration	Global Alexa Page ranking
Cake Financial	Investing		Open	
Care2	<u>Green</u> living and social activism	9,961,947	Open	
Classmates	School, college, work and the military	50,000,000	Open	923
Cloob	General, popular in Iran		Open	
College Tonight	College students		requires an e-mail address with an ".edu" ending	
CouchSurfing	Worldwide network for making connections between travelers and the local communities they visit.	871,049	Open	
CozyCot	Social networking site for women from South East Asia (especially Singapore), East Asia, North America, and Australia		Open	41,516
DeviantART	Art community	9,040,962	Open	119
dol2day	Politic community, social network, internet radio (German-speaking countries)	40,200	Open	
DontStayIn	Clubbing (primarily UK)		Open	
Elftown	Community and wiki around fantasy and <u>sci-fi</u>	185,000	Open, approval needed	
Epernicus	For <u>research scientists</u>		Open	
Eons.com	For <u>baby boomers</u>		Open to people 13 and older	13,675
Espinthebottle	Teen networking site offering photos, games, and relationships		Open to people 13 and older	
Experience Project	Life experiences		Open	
Facebook	General	175,000,000	Open to people 13 and older	5
Faceparty	General, popular UK	200,000	Invitation only to people 18 and older	2,481
Faces.com	British teens		Open to people 13 and older	
Fetlife	People who are into BDSM	32,500	Open to people "of [legal] age to see adult content"	54,198
Filmaffinity	Movies and TV series	250,000	Open	4,082



Name	Description/Focus	Registered users	Registration	Global Alexa Page ranking
Flixster	Movies	63,000,000	Open to people 13 and older	309
Flickr	Photo sharing, commenting, photography related networking, worldwide		Open	37
Fotolog	Photoblogging. Popular in South America and Spain.	20,000,000	Open	57
Friends Reunited	UK based. School, college, work, sport and streets	19,000,000	Open	8,052
Friendster	General. Popular in ASEAN countries.	90,000,000	Open to people 16 and older.	35
Frühstückstreff	General		Open	
Fubar	dating, an "online bar" for 18 and older	1,200,000	Open	2,609
Gaia Online	Anime and games		Open to people 13 and older	
Gather	Article, picture, and video sharing, as well as group discussions	465,000	Open	
Geni.com	Families, genealogy	15,000,000	Open	
Goodreads	Library cataloging, book lovers		Open	5,305
Gossipreport.com	Anonymous gossip		Open to people 16 and older	
Grono.net	Poland		Open since 2009	
Habbo	General for teens, over 31 communities worldwide, <u>chat room</u> and user profiles.	117,000,000	Open to people 13 and older	4,050
hi5	General, popular in Angola, Portugal, Cyprus, Romania, Thailand, Central Africa, and Latin America	80,000,000	Open to people 13 and older	16
Hospitality Club	Hospitality	328,629	Open	
Hyves	General, Most popular in the <u>Netherlands</u>	8,000,000	Open	216
imeem	Music, Video, Photos, Blogs	24,000,000	Open	140
IRC-Galleria	Finland	505,000	Open to Finnish speaking people 12 and older	
Italki	Learning languages, and helping others to learn	350,000	Open	
InterNations	International community		Invite-only	30,147



Name	Description/Focus	Registered users	Registration	Global Alexa Page ranking
itsmy	Mobile community worldwide, blogging, friends, personal TV-shows	2,500,000		
iWiW	Hungary	1,700,000	Invite-only	
Jaiku	General, owned by Google		You must request an invitation into the beta-test	
Jammer Direct	Creative resource website		Open to the General Public	
kaioo	General, nonprofit	30,000		
kaixin	General, in simplified Chinese; caters for mainland China users		Open to the General Public	
Last.fm	Music	21,000,000	Open to people 13 and older	262
LibraryThing	Book lovers	400,000	Open to people 13 and older	
lifeknot	Shared interests, hobbies		Open to people 18 and older	
LinkedIn	General but mainly business	35,000,000	Open	192
LiveJournal	Blogging	17,564,977	Open (OpenID)	56
Livemocha	Languages, used to learn and help others learn languages	1,000,000	Open	5,505
LunarStorm	Sweden		Open	
MEETin	General		Open	
Meetup.com	General, used to plan offline meetings for people interested in various activities		Open to people 18 and older.	
Meettheboss	Business and Finance community, worldwide		Open	
Mixi	Japan	20,936,509	Invite-only	64
mobikade	Mobile community, UK only		Open to people 18 and older	
MocoSpace	Mobile community, worldwide	3,000,000	Open to people 14 and older	
MOG	Music		Open to people 14 and older	
Multiply	"Real world" relationships	10,000,000	Open to people 13 and older	150
Muxlim	Muslim portal site	50,000	Open to people 13 and older	94,338
MyChurch	Christian Churches	144,295	Open	33,621



Name	Description/Focus	Registered users	Registration	Global Alexa Page ranking
MyHeritage	Family-oriented social network service		Open	
MyLOL	General, popular in the United States, Europe and Australia	32,000	Open to ages 13 and up	253,145
MySpace	General	253,145,404	Open to ages 14 and up	6
myYearbook	General	5,100,000	Open to age 13 and up & Grades 9 and up	894
Nasza-klasa.pl	School, college, and friends, popular in Poland	12,000,000	Open	
Netlog	General, popular in Europe and Québec province. Formerly known as Facebox and Redbox	42,000,000	Open to people 13 and older	98
Nettby	Norwegian community		Open	
Nexopia	Canada	1,400,000	Open to people 14 and older	4,362
Ning	Users create their own social websites and social networks		Open	566
Odnoklassniki.ru	General, popular in Russia and former Soviet republics	30,000,000	Open	42
OkCupid	Social networking and dating		Open to people 18 and older	
OneWorldTV	<u>Not for profit</u> video sharing and social networking aimed at people interested in social issues, development, environment, etc.		Open	
Orkut	Owned by Google. Popular in Brazil, Paraguay, India, Pakistan and Estonia.	67,000,000	Open to people 18 and older, (Google login)	11
OUTeverywhere	Gay/ <u>LGBTQ</u> Community		Open	
Passportstamp	Travel		Open	
Pingsta	Collaborative platform for the world's <u>internetwork experts</u>		Invite-only, only Internet Experts	
Plaxo	Aggregator	15,000,000	Open	
Playahead	Swedish, Danish, Norwegian teenagers		Open	
Playboy U	Online college community		Open to college students with .edu e-mail address	
Plurk	Micro-blogging, RSS, updates		Open	27,061



Name	Description/Focus	Registered users	Registration	Global Alexa Page ranking
quarterlife	A social network for artists, filmmakers, musicians, and creative people		Open to people 14 and older	
Ravelry	Knitting and crochet	270,000	Invite-only while in beta	
Reunion	Locating friends and family, keeping in touch	51,000,000	Open	2,311
ResearchGATE	Social network for scientific researchers	25,000	Open	
Reverbnation	Social network for musician and bands	25,000	Open to people 16 and older	
Ryze	Business	500,000	Open	
scispace.net	Collaborative network site for scientists		By invitation, but can request an invitation	
Shelfari	Books		Open	
Skyrock	Social network in French-speaking world	22,000,000	Open	41
SocialVibe	Social network for Charity	435,000	Open	
Sonico	General, popular in Latin America and Spanish and Portuguese speaking regions	17,000,000	Open to people 13 and older	297
Soundpedia	Music		Open	154,672
Spoke	Business networking		Open	5,568
Stickam				
Live video streaming and chat.	2,000,000		Open	
StudiVZ	University students, mostly in the German-speaking countries	8,000,000	Open	
Tagged	General	70,000,000	Open	94
Talkbiznow	Business networking		Open	395,824
Taltopia	Online artistic community		Open	
TravBuddy	Travel		Open	
Travellerspoint	Travel		Open	
tribe.net	General		Open	3,517
Trombi	French subsidiary of Classmates.com	4,400,000		
Tuenti	General, very popular in Spain		Invite-only	587
Twitter	Micro-blogging, RSS, updates	2,200,000	Open	599



Name	Description/Focus	Registered users	Registration	Global Alexa Page ranking
V Kontakte	Russian social network	30,005,000	Open	27
Vampirefreaks	Gothic and industrial subculture	1,931,049	Open to users 13 and over	
Viadeo	European social networking and campus networking in seven languages	6,000,000	Open	
Vox	Blogging		Open	1,549
Wasabi	General		Open	
WAYN	Travel and lifestyle	10,000,000	Open to people 18 and older	823
WebBiographies	Genealogy and biography		Open	
Windows Live Spaces	Blogging (formerly MSN Spaces)	120,000,000	Open	4
Wis.dm	Questions and answers about anything and everything	50,000	Open	
WiserEarth	Online community space for the social and environmental movement	20,600	Open to people 18 and older	114,942
Xanga	Blogs and “metro” areas	27,000,000	Open	230
XING	Business (primarily Europe (Germany) and China)	6,000,000	Open	1,814
Xiaonei	Significant site in China	15,000,000	Open	
Xt3	Catholic social networking, created after World Youth Day 2008		Open	
Yelp, Inc.	Local business review and talk		Open	
Youmeo	UK social network (focus on data portability)		Open	
Zoo.gr	Greek web meeting point	890,000	Open	5,634