

Preventing Cyberbullying

A Guide to Safe and Responsible
Internet Use in the Digital Age

EdgeWave

15333 Avenue of Science
San Diego, CA 92128.

Phone: 858-676-2277

Fax: 858-676-2299

Toll Free: 800-782-3762

Email: info@edgewave.com

www.edgewave.com

Schools and Social Networking

The digital age has brought many advances that have connected us globally like never before. Among the advantages to educators are the expansive resources now available to them that can enrich the learning environment, engage and motivate students and offer more convenient modes of communication to everyone. Benefits range from having access to resources such as the YouTube for Schools service, which delivers hundreds of age-appropriate education videos to schools all over the country, to the ability for individual teachers to set up their own classroom blogs or websites, where they have a venue for posting announcements and homework assignments and in general, establishing a forum for communicating with students on and off-campus.

However, social media sites also have a more ominous side. Stories of minor students being exposed to inappropriate material, sexual predators, and bullying and harassment by peers are becoming all too common.

This white paper attempts to explain the issues surrounding social networking among K-12 students and discusses some of the risks schools are facing as they try and contend with the virtually unanimous participation in social media among students. It will examine statistics around student use of social media technology and present some of the risks involved, including cyberbullying. The paper explains the types of cyberbullying that are occurring and how victims can suffer long-term damage as a result. It concludes with a discussion of why experts recommend social networks not be banned in schools and offers practical steps schools can take to manage student online interactions at school and at home. Finally, it offers a solution that gives schools the granular control required to make social media tools safe for students. One that gives schools visibility into and control over social media interactions, to not only help them educate students in the proper use of social media, but to help prevent problems such as cyberbullying and other inappropriate activities.

New FCC Rules on Social Media Impact CIPA

One recent development that is going to impact how schools handle social media is an order released by the Federal Communications Commission in 2011 called the Protecting Children in the 21st Century Act. This legislation has expanded CIPA rules to include social media applications such as Facebook, MySpace and YouTube, tying them to E-Rate funds that schools count on for much needed technology acquisitions. Schools must comply with these rules by July 1, 2012.

The new Act requires that school district policies include the instruction of minors in the safe and appropriate use of social networking sites and chat rooms, with the goal of providing direction to students concerning their behavior when interacting with others on social media sites.

Compliance with the new rules will directly affect the distribution of E-Rate funds. And like CIPA, schools will have to put policies in place to prove they are abiding by the new rules.

Here is a summary of the new FCC Rules stipulations:

- The new requirements are in addition to existing Children's Internet Protection requirements including Internet filtering technology, staff, student and parent education, etc.
- In addition to mandating policies, the FCC specifically points to sites such as Facebook and YouTube and confirms that these sites are potentially harmful to minors but not harmful in and of themselves.
- Social networking sites do not fall into the category of websites that must be blocked
- The FCC acknowledges that social networking sites may have the potential to support student learning

The FCC stated that by the July 1st deadline, "School Boards will have to create or update current Internet Use policies to include wording that they are teaching Internet safety".

Schools are also encouraged to provide education and training not only on the appropriate use of these sites but on their potential for enhancing the learning experience.

The new rules are impacting how schools approach social media use by students and emphasize the need to better manage the

dangers inherent in the rampant adoption of social networking tools by students nationwide. One of the most serious problems facing schools is the prevalence of cyberbullying, which this paper will discuss in more detail.

Cyberbullying - An Old Problem Wrapped in New Technology

The tragedies associated with cyberbullying have been publicized for all to read. While the Internet is proving to be a boon for schools with services such as YouTube for Schools and other scholastic sites, not to mention the ability for teachers to communicate with their students, post homework assignments and course material, and provide other resources online, there is a downside. In this case, it's a serious one and it's called cyberbullying.

Of course, the school bully is an almost iconic image, portrayed in books and movies since the advent of educational institutions. But where one bully might terrorize one or two peers in his neighborhood or classroom, he or she now has access to a vast audience, with the ability to humiliate the victim on a scale never before possible. Even worse, the bully can now pursue his or her damaging behavior behind a cloak of anonymity, something that was far less feasible before the Internet. And while bullies can exist anywhere, the most vulnerable victims are children. According to the Center for Disease Control, which characterizes cyberbullying as electronic aggression, "Young people who are victims of internet harassment are significantly more likely than those who have not been victimized to use alcohol and other drugs, receive school detention or suspension, skip school, or experience in-person victimization."

Cyberbullying is in the News

Cases of student harassment and violence resulting from social media postings are all too common:

- At a central Indiana high school, an anonymous Facebook page called the "Burnbook" has translated into violence. The site has been used to post rumors, insults and even threats of physical violence between students resulting in fear and unrest on the school grounds. The page was brought to the attention of school officials by a concerned parent.
- A Myspace feud between two 13-year-old girls at a Cleveland middle school resulted in gunfire with bullets grazing the ear of one of the students as she sat in a car in front of her house.

Even more tragic are the student suicides resulting from cyberbullying – just a few examples include:

- A 17-year-old Kentucky high school student committed suicide after receiving a series of threats and intimidating messages from an anonymous MySpace page. The final message leading to her death was "I am not going to put you in the hospital; I am going to put you in the morgue."
- A 15-year-old Florida student was bullied online for three years before taking his own life. After his death, his mother, who was a teacher, worked to get the Florida legislature to pass anti-bullying laws. Similar laws have been passed or are being considered in scores of other states.
- In Vermont, a 13-year-old middle school boy, who was bullied from the age of 11, took his own life after the bully spread anonymous online rumors that he was gay. His father said he could have withstood the harassment if it had occurred before there was an Internet.

General Statistics for Online Activity Among K-12 Minor Students

Studies show that participation by children and teens in online activities continues to grow. Pew Research Center surveyed over 2400 parent-child pairs in their Internet and American Life Project. The children were between the ages of 12 and 17. The following statistics are the result of these nationally conducted interviews done over a multi-year period from 2007 to 2010:

- 95% of all teens surveyed use the Internet on a regular basis, and 80% of them use social networking sites
- 94% of students surveyed said they go online to do research for school assignments with 48% saying they do so most days

- 81% say they visit sites for information about movies, TV shows, music groups or sports stars
- 73% of the teens stated that they are users of online social networking sites, with 37% saying they send daily messages via social media
- 64% of students who are online revealed that they have created online content of some kind
- 62% stated they visit websites to get news
- 57% have watched a video on a video-sharing site such as YouTube or GoogleVideo
- 55% go online to get information about a college, university or other school they are considering attending
- 49% have purchased something online like books, clothes or music
- 31% have looked online for health, dieting or physical fitness information, while 17% have looked online for sensitive health information

Using this data, we can come to a fairly concrete conclusion that students are online frequently and that the much of their time is spent in positive activities. Students may be researching homework assignments, or visiting college sites for information or, may be checking out the website of their favorite movie or band. It's clear that there is a positive side to online behaviors – even those involving social networking. However, it does not diminish the fact that serious harm has been caused by the large presence of social media in the lives of young people. Parents and schools need to be aware of the dangers and mitigate the risks before terrible events happen.

Cyberbullying: The Darker Side of Student Online Behavior

The Center for Disease Control (CDC) defines cyberbullying or electronic aggression as “Any type of harassment or bullying (teasing, telling lies, making fun of someone, making rude or mean comments, spreading rumors, or making threatening or aggressive comments) that occurs through email, a chat room, instant messaging, a website (including blogs) or text messaging.” Experts point out that it is the “repeated” instances of spreading rumors or other harmful content that constitutes true cyberbullying.

In the Pew survey of online behavior of 12-17 year-olds, they reported the following:

- 32% of the teens surveyed reported being the targets of a range of troubling and/or intimidating online activities from their peers or anonymous sources:
 - 15% said that a private message they had written was posted or forwarded without their permission
 - 13% reported that someone was spreading rumors about them online
 - 13% said they had received a threatening or aggressive message from someone
 - 6% said embarrassing pictures of them had been posted online
- 38% of girls say they were bullied online, while 26% of boys reported they had been. Girls in the 15-17 age group reported the most bullying – 41% -- more than any other group
- For the teens who use social networking sites, 39% reported being cyberbullied compared to 22% of teens who don't engage in social media activities
- Of teens who use social media, 88% report that they have witnessed someone being mean or cruel to another online, with 12% saying this is a 'frequent' occurrence.
- Bullying still occurs at school more often than online but the survey also showed that students who are cyberbullied are

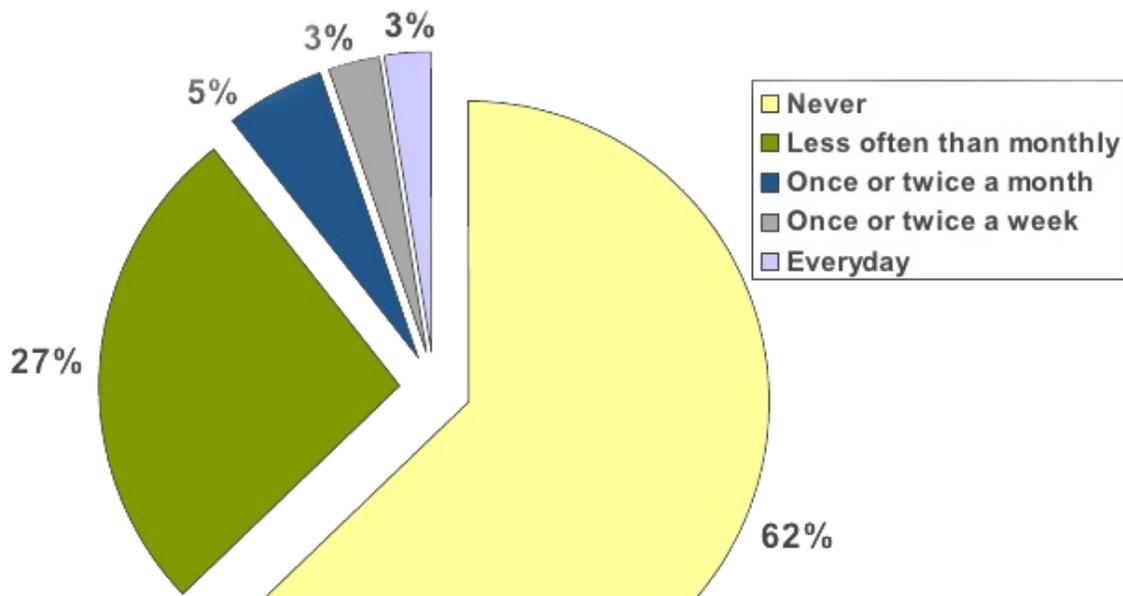
Cyberbullying is a Growing Trend

Recent data compiled by the website Internet Safety 101 report that 43% of teens aged 13 to 17 say they have experienced some sort of cyberbullying in the past year.

more likely to also be bullied at school

- Parents at a rate of one in six say they know that their child has been bullied on social media sites and in over half of these cases, their child was bullied multiple times.
- Of students considered heavy users of social networking, those who spend more than three hours per school day on social media sites, the study found them 110% more likely to be a victim of cyberbullying

Frequency of bullying victimization among 11-16 year olds



Types of Cyberbullying

Although the Internet has many sites devoted to cyberbullying including school sites, research organizations that monitor and study the problem and other resources, there is some agreement on the general forms, cyberbullying can take. Here is summary:

Gossip – A pastime as old as humanity, for teens, who have less experience and resiliency, gossip can be devastating. This form of cyberbullying includes posting to social media sites or sending cruel gossip aimed at damaging someone’s reputation and relationships with friends, family and acquaintances.

Exclusion – Particularly painful during formative teen years, this involves deliberately excluding someone from group activities.

Falsifying Identity – This occurs when the offender hacks another’s account and begins posting content or pictures aimed at causing embarrassment or reputation damage to the victim, often resulting in isolating the victim from others.

Harassment – In cyberbullying, this involves posting or sending rude, offensive and insulting comments or posting them repeatedly.

Cyberstalking – This involves repeated posting or sending of annoying or overfamiliar messages or other inappropriate content

Flaming – If you read the comments section of almost any news story, particularly controversial ones, you might conclude that angry, derisive or otherwise insulting content has become the norm. When children are involved this sort of activity can engender fear and anxiety.

Deception and/or Outing – Using deceptive means to trick others into revealing private or embarrassing information and then revealing it on social networking sites can be devastating for teens. Although this sort of thing has occurred before there was an Internet, the ability to make this information universally available via social networking has increased its potential damage exponentially.

Cyberthreats – The statistics compiled by Pew also showed that children and teens who are harassed online are more likely to be harassed offline. Threats can include those against another where bodily harm is threatened or students who exhibit suicidal tendencies in their online posts and messages.

Cyberbullying Causes Lasting Damage

The characteristics that are inherent on cyberbullying are also the ones that can make it a particularly damaging threat. Because the offensive and harmful contact is online, the content can be preserved and transmitted, re-inflicting the insults and humiliation over and over. Also, bullying events that occur on school grounds may be witnessed by one or a few kids, but in cyberspace, the audience is limitless – increasing the victim's humiliation and suffering. Other factors including the familiarity with victims that bullies may use can make their exploits particularly personal and painful and also the speed at which harmful content can reach an audience makes damage control nearly impossible. With access to social networking sites such as Facebook and Twitter, bullies now have a venue that gives them almost limitless access to support for their insults, rumors and threats. The insults, comments or images can be preserved by the person who was bullied or by others so that the victim may read or view them over and over again and the harm is re-inflicted with each reading or viewing.

According to psychologists, the damage inflicted on victims of cyberbullying can follow them into adulthood resulting in lasting low self-esteem and increased risk for addictions, poor job performance and other maladaptive behaviors.

Cyberbullying can Result in Lawsuits for Schools

Since almost all states have laws against bullying on the books, some cases of cyberbullying that involved the deaths of students have resulted in costly lawsuits against schools and school districts. Some have resulted in court cases and many more were settled out of court. A few examples include:

- In Louisiana a school board is being sued over the death of a 15-year-old girl who committed suicide after enduring months of cyberbullying by classmates. The parents contend that her school did nothing to stop the vicious attacks even when they were made aware of the situation.
- In an infamous case in Massachusetts, the parents of a 15-year-old-girl who killed herself after being cyberbullied by classmates for months, sued her school and settled the case out of court. The high school agreed to pay hundreds of thousands of dollars to the victim's family for their failure to intervene in her victimization.
- Parents of middle school student in Boca Raton, FL are suing the school over its failure to protect their son from bullying. They had been pleading with the school administration since 2010 to take action and were finally forced to pull their son from the middle school and are now home-schooling him.

States are Passing Laws to Address Cyberbullying Specifically

Because of the prevalence and extreme nature of many cyberbullying instances; states have been compelled to instigate legislation that often impacts schools directly. Of the 49 states that either have or are proposing anti-bullying legislation, 44 of them include language aimed at "electronic harassment" and 21 of them include stipulations specifically citing "cyberbullying". And all of the states with anti-bullying laws require that schools put policies in place to back up the legislation.

The fact that some school districts have been sued when cyberbullying has led to violence either between students, or students



Young people who are victims of internet harassment are significantly more likely than those who have not been victimized to use alcohol and other drugs, receive school detention or suspension, skip school, or experience in-person victimization."

Center for Disease Control

taking their own lives, is making it clear that schools need to take control over this pandemic situation. Here's an overview of current state laws involving cyberbullying at schools:

Every state but Montana has anti-bullying laws, but more and more states are expanding or updating their laws to address cyberbullying specifically.

States that have expanded anti-bullying laws to include cyberbullying or where it is proposed: Georgia, Illinois, Kentucky, Maine, Nebraska, New York, Arkansas, California, Connecticut, Hawaii, Kansas, Louisiana, Massachusetts, Missouri, Nevada, New Hampshire, North Carolina, Oregon, Utah, Washington

States that require, or have a proposal to require a school policy addressing cyberbullying: Georgia, Illinois, Kentucky, Maine, Nebraska, New York, Arkansas, California, Connecticut, Hawaii, Kansas, Louisiana, Massachusetts, Missouri, Nevada, New Hampshire, North Carolina, Oregon, Utah, Washington

All states that have anti-bullying laws, (and that's every state except Montana) allow schools to discipline students for off-campus bullying.

Some of the states that are addressing cyberbullying also allow discipline for off-campus cyberbullying offenses, they include: Georgia, Nebraska, New Jersey, South Dakota, Arkansas, Connecticut, Louisiana, Massachusetts, New Hampshire

The adoption of these new laws, with specific language addressing cyberbullying and electronic harassment may make schools and districts more vulnerable to lawsuits when they fail to initiate the policies and protections required to keep students from being victimized. By including off-campus discipline, states are attempting to mitigate the risks associated with the ubiquitous presence of social media in students' lives.

These states will mandate schools to take action when the law is present, but even in states without specific cyberbullying laws, schools will need to find solutions in order to maintain student safety.

Steps Schools Can Take to Combat Cyberbullying

Step One: Know Cyberbullying when You See It

It can be difficult to discriminate between the innocent teasing in which children typically engage, and the truly mean and hurtful banter that can escalate into cyberbullying. Research indicates that middle school girls are particularly prone to this sort of bullying and are also at a vulnerable stage where rumors, insults and other mean comments can be the most damaging. Research also shows that cyberbullying can generate physical violence on school grounds, particularly when it involves boys. That's why the CDC and many of the standing and pending state laws characterize "electronic aggression" or cyberbullying as an act of violence. Schools need to be aware of students' online activities so that when they see an early or potential cyberbullying event unfolding, they can act quickly to stop it. Because cyberbullying can remain anonymous, the bully feels emboldened by the ability to keep his or her identity concealed. It's important that victims and their parents be heard and that their claims be thoroughly investigated so that the cyberbullying can be stopped.

Make sure teachers and staff are aware of the types of cyberbullying they might encounter and what signs of trouble they should be looking for. The school psychologist and guidance counselors can be excellent resources for this information. If teachers detect a student they feel might be involved in or a victim of cyberbullying, give them clear guidelines about who to alert and how to proceed to handle the situation.

Step Two: Have Strong Policies in Place

The new FCC/CIPA rules addressing cyberbullying specifically, call for schools to not only establish acceptable use policies regarding social networking, but to train teachers, staff and students as to what the policies are. In addition, schools are required to establish training that will result in students becoming humane and mature users of social media so that cyberbullying is less likely to occur. Make sure your policy is comprehensive and that it addresses all forms of social media -- social networking sites, Twitter, blogs, IM applications, peer-to-peer and texting. If your school is in a state where discipline of off-campus behavior is allowed, you should address those points in your policy. Even if a state has not specifically addressed cyberbullying in its laws, schools are finding it

important to take steps to assure students are protected. Adopt a zero-tolerance policy towards cyberbullying and make sure students and parents understand the gravity of the problem. They should also be given a clear explanation of the consequences for anyone caught engaging in bullying other students, whether on or off-campus.

Step Three: Train Students and Staff

Training is a mandatory part of the new FCC/CIPA rules and also included in many of the state laws on cyberbullying. The goal of the legislation is to encourage schools to establish programs that will result in modifying student social networking behavior. Any schools wishing to comply with CIPA will need to make sure such training happens in their schools. Of course, complying with CIPA is only one benefit of such a program, of even greater value is that training students to be good social networking citizens will help prevent cyberbullying – what this legislation and others throughout the country hope to achieve.

Training should be formalized across grade levels and conducted more than once during the school year. What is clear in the new rules and most state-level legislation is that schools are not expected to simply block and ignore social media venues at school and consider the job completed. The rules acknowledge that a vast majority of students are engaging in social networking activities -- Facebook, Twitter, YouTube, FourSquare, blogs, and dozens of others. The sooner schools can produce students who will use social media responsibly, the less they will have to worry about cyberbullying and other inappropriate online behaviors.

Professional development for teachers, administrators and staff should be part of your training program. Teachers should be familiar with what social media sites their students are using and understand the ethical, legal and practical issues associated with social networking and mobile devices in the classroom. Their training should include how to convey this information to students as part of their daily instruction and use of social media tools.

Teachers and staff also need to recognize signs of cyberbullying and other inappropriate behavior among their students. Many children who are in trouble will exhibit signs of their despair on social networking sites well before violence or an irreversible tragedy can occur. Educators need to look for the signs of cyberbullying and be able to detect when innocent teasing or a student's sad postings seem to be taking a darker turn.

It's also important that schools keep parents informed and in particular, alert them if they suspect a student is either the victim or perpetrator of cyberbullying.

Step Four: Include Technology to Assure Enforcement

Rules and regulations are inadequate without a way to enforce them. Though some schools have chosen to block social networking activity among students completely, others take a more realistic approach and look for ways to monitor student social networking use in order to prevent problems. It is also difficult to train students to use social media appropriately, if they are not allowed access to sites at all.

Why Blocking Access to Social Media is Not the Answer

In December of 2011, a group of senior-level representatives from state and national organizations met to discuss social media in schools. The result of their meeting was a comprehensive report entitled, "Making Progress: Rethinking State and School District Policies Concerning Mobile Technologies and Social Media". The creators of this report did not define it as a prescription policy statement but rather a document designed to "inform policymakers and educators as they develop or reconsider policies addressing new digital media in the context of improved learning". This report is already having an impact on schools with more than a dozen prominent national educational and ed-tech groups releasing this report to their constituents.

The report relied on the Pew Research Center study previously referenced in this paper. A major conclusion of this study was that banning social media in schools is not the answer.

The report supported this by pointing out that technology has made mobile devices and social media available to K-12 students and that educators are realizing their value and embracing them because they allow students to:

- Bridge the gap between formal in-school learning and informal out-of-school learning which can improve their preparedness for real world experience

- Build their own learning environments that will help them achieve academically and acquire the skills they need for the 21st century. These tools allow them to connect instantly with peers, experts, and information resources beyond the school walls.
- Provide real-time feedback, exchange information and receive assessments during classroom instruction through text messages or Twitter
- Document and record their work with images taken on and off campus
- Receive and submit homework assignments digitally and learn how to use mobile devices and social networking tools to pursue lifelong learning

The study also acknowledged the dangers inherent in these tools in the hands of students and recommended that schools adopt policies and acquire the means to protect students from dangers such as inappropriate content, predators, student immaturity, and cyberbullying.

The study concludes with recommendations that coincide with the steps outlined in this paper; create strong policies, educate students, establish professional development resources for teachers and staff and above all, not to ban the use of social media in schools because it not only deprives students and teachers of valuable learning resources, but due to its ubiquitous use among students, may postpone the inevitability of having to manage and control social media use among students.

iPrism Social Media Security – A Granular Approach to Social Networking Safety

EdgeWave offers iPrism Social Media Security, which allows schools to take advantage of educational resources offered by social media tools, while protecting students from the pitfalls of inappropriate content, cyberbullying and distracting non-school related usage.

iPrism's unique Social Media Security solution provides granular control over social networking applications such as Facebook and Twitter, and helps educators promote the responsible use of social media that can enrich the classroom experience and enhance learning.

As an add-on to the popular iPrism Web Security solution, Social Media Security is easy to deploy and manage. As a cloud-based solution, it is easily scalable and customizable to conform to any school requirement.

iPrism Social Media Security:

- Allows students full access to popular social media applications while keeping their interactions consistent with CIPA requirements and your school's acceptable use policies
- Gives schools visibility on the social media interactions of students so that signs of cyberbullying, self-harming or other damaging activity can be detected early and mitigated
- Eliminates the transmittal or posting of inappropriate content, including cyberbullying, in news feeds, posts, blogs and messages while making acceptable content available
- The policy management interface gives administrators granular control of social media content at the application level for real-time control over social media activity via the school network
- Users who try to post inappropriate or hostile content will receive a customizable block message from within the application itself, preventing the bad action from occurring
- iPrism Social Media Security includes many out-of-the-box templates which can be used as is, or customized to fit each school's requirements
- The service integrates seamlessly with iPrism Web Security through the central management interface for easy deployment and management

- Includes comprehensive drill-down reporting to provide school officials with an accurate picture of social media interactions by students and staff across schools or school districts

About EdgeWave

EdgeWave™ develops and markets innovative Secure Content Management (SCM) solutions including iPrism Web Security and the ePrism Email Security Suite with next generation solutions for Email Filtering, Continuity, Data Loss Protection, Encryption and Archive. EdgeWave innovative technologies deliver comprehensive protection with unrivalled ease of deployment and the lowest TCO on the market. The company's award winning solutions can be delivered as hosted, on-premises, and hybrid services.