



Safety and Security in Web 2.0 Learning Environments

Education Thought Leadership Series

Embracing Web 2.0 tools and integrating them into our schools and learning environments present new challenges that require flexible and proactive solutions. To adhering to regulatory compliance and keep students, data, and networks safe in a Web 2.0 world, three critical areas need to be addressed: cyberethics, cybersafety, and cybersecurity. Cyberethics requires strategies to educate both staff and students on proper and safe Internet use and is addressed by the Protecting Children in the 21st Century Act. Cybersafety, with regard to student and staff use, is included in the Children's Internet Protection Act (CIPA).¹ Cybersecurity of data and information is included in the Family Educational Rights and Privacy Act (FERPA).² This paper provides examples of the challenges faced by education leaders, along with solutions and strategies to meet regulatory compliance through best practices research.

When the Internet was first used for education, the Web was predominantly used to research information and access sources not previously available to most students. At that time, the primary goal of student safety was to ensure that users did not view or access inappropriate content and that downloaded information was free of viruses or other malware. The introduction of Web 2.0 into education brings a more complex set of challenges that require various strategies to protect students from interacting with inappropriate content and Web users and keep data, networks, and infrastructure secure from external attacks.

CYBERETHICS

With respect to Cyberethics, the National Cybersecurity Alliance recently surveyed 1,003 teachers, 400 school administrators, and 200 technology coordinators from U.S. schools and gathered interesting results³:

- Most teachers and technology coordinators believe that parents are primarily responsible for teaching children about Internet safety, while school administrators are most likely to think teachers/schools are responsible.
- School administrators and technology coordinators are more likely than teachers to believe that their school/district adequately educates students regarding cyberethics, safety, and security issues, yet only 50% of teachers feel prepared to discuss cyberbullying.
- More than half of administrators and technology coordinators agree their school/district requires cyberethics, safety, and security curriculum to be taught in the classroom setting, yet only a third of teachers agree.

Additionally, *The State of K-12 Cyberethics, Cybersafety, and Cybersecurity Curriculum in the U.S. Survey* reports that, "America's young people aren't receiving adequate instruction to use digital technology and navigate cyberspace in a safe, secure, and responsible manner and are ill-prepared to address these subjects." The report further cites that, "Seven in ten teachers think cyberethics, cybersafety, and cybersecurity training should be a high priority in their professional development needs." This topic should be addressed mainly through professional development for our K-12 educators and by educating our students. A number of free resources for teacher professional development and student education are included in the Additional Resources section at the end of this document.

CYBERSAFETY

Educational leaders across our nation place child safety at the very top of their priority list. Each school day, parents entrust their children to the care of teachers, administrators, paraprofessionals, and a vast network of school support staff. School leaders are responsible for ensuring that students are safe from both physical and emotional dangers. Access to the Internet in the school setting has presented a new safety challenge for educators. The federal Children's Internet Protection Act (CIPA)⁴, established in 2001, requires that schools and libraries receiving E-rate funds must certify that they have an Internet safety policy that includes technology measures to protect students' privacy and safety. CIPA was an important first step in requiring schools to proactively institute Internet protection policies and strategies to keep students safe from inappropriate content on the Web. Educational technology leaders understand that CIPA compliance is only one component of a more complex solution required to provide online student safety.

CYBERSECURITY

Few district IT leaders realize the degree to which malware attacks are occurring through the Web, a recent shift in the threat landscape. The increased use of Web 2.0 tools for teaching and learning has made proactive Web security an organizational imperative. The following statistics, according to the latest research from M86 Security Labs, cannot and should not be ignored:

- 92% of new malware threats come from the Web
- 84% of Web malware comes from legitimate Web 2.0 sites

Because social networking tools are used in the classroom more often, the associated risks are a major concern for technology directors. Furthermore, legislation such as the Family Educational Rights and Privacy Act (FERPA) requires that education IT leaders protect the personal data stored about students, families, and staff from inappropriate access and/or distribution. Examples of the Web 2.0 environment posing potential security risks to data, personal information, and network infrastructures include global classroom projects, virtual reality, streamed media, and e-commerce.

- The Flat Classroom™⁵ is an example of a global collaboration project for middle and high school students that partners classrooms from around the world to research and discuss topics related to new and emerging technologies. The project uses Web 2.0 tools such as wikis, blogs, and video conferencing to enable students to learn together in real time.
- Second Life® is a virtual reality application with growing application to education. In a high school health class, for example, students create Avatars reflecting how they see themselves, opening a discussion on self-perception and improving one's self-image.
- YouTube.com contains a number of educationally valuable videos as well as many that would be inappropriate for student viewing. For example, the video "How it Feels to Have a Stroke"⁶ provides personal experience from a neurological expert that would support any biology or anatomy class.
- E-bay and Craig's List are popular sites that help school administrators recover funds by selling outdated textbooks and equipment. While the revenues are sorely needed, the opportunities for fraud is abundant.

To address cybersecurity concerns, IT leaders need to focus on ways to institute policies, procedures, and applications that protect users, data, and the network. This paper explores the factors involved in child safety, network protection, and regulatory compliance as a part of the M86 Education Thought Leadership series. It outlines approaches that are available to keep our students safe while enabling them to use exciting Web 2.0 tools and Internet resources to learn and explore. Those responsible for developing district IUP/AUP guidelines and implementing Internet safety and security solutions will find this document enlightening, engaging, and informative.

STUDENT SAFETY IN THE WEB 2.0 CLASSROOM

The atmosphere was tense as the principal strode in and summoned two students to his office. A few minutes later, Adam and Zack found themselves sitting across from the principal, the dean of students, and the technology coordinator. Projected on the whiteboard was a Facebook page for "Sandra", an unpopular girl in the school, featuring dozens of unflattering pictures, an inaccurate profile, and a "wall" full of profanity, insults, and threats. A posted event listed the following day as "Get Sandra Day". It appears that Adam

and Zack had used one of the school-provided netbooks at home the previous evening to create "Sandra's Facebook" page. Luckily all the school computers, even the mobile units that students are allowed to take home for completing assignments, have remote Web filtering and monitoring. The graphics and inappropriate language triggered the real-time mitigation and "locked out" the students' ability to post the offensive Facebook page. Sandra would not be embarrassed and school staff has the information they need to investigate this potential bullying incident before it escalates any further. Adam and Zack realized the consequences of breaking the district's Acceptable Use Policy, as it was easy for the IT staff to document the infraction.

In Massachusetts, community members are struggling to explain the death of a 15 year-old girl who was bullied to the point of hanging herself⁷. Additionally, two high school students are charged with criminal harassment after creating a YouTube video mocking a student with special needs, and three 14 year-olds are being charged with identify theft for creating a social networking page about another victim^{8,9}. With the increased availability of instant communication in the form of email, instant messaging, text messaging, blogs, chat rooms, and other social networking sites, spontaneous action/reaction is becoming the norm. Unfortunately, once these thoughts are posted, they are difficult, if not impossible, to retract.

Working to Halt Online Abuse (WHOA) is a volunteer Internet safety organization that helps victims of cyberstalking. They report a significant increase in cyberstalking over the previous year and a narrowing of the gap between male and female victims. The report cites an increase in Asian and African American victims and an increase in victims who do not live in the same state as their assailant¹⁰. The criminal justice and legal systems are just beginning to catch up with cybercrimes and cybercriminals, yet school and district leadership is required to address these issues now.

Some technology directors handle these "risky" Web sites by blocking them all, while others creatively apply filters, access rights, and monitoring technologies to control who is allowed to connect to these sites. Long term, the availability of these sites will increase. It is important that students and teachers observe network safety rules and behave responsibly on the Internet, as technology directors implement solutions that allow access to the educational content in the Web 2.0 space.

Providing access to Web 2.0 resources that the "digital natives" in our K-12 classrooms find so engaging is one of the greatest challenges of IT leaders in schools nationwide. Developing strategies and solutions that protect without inhibiting the creative and appropriate use of blogs, wikis, social networking sites, and simulated worlds requires collaboration, planning, and trust.

For more information on CIPA compliance strategies and cyberbullying, please refer to the M86 Security white paper, **Cyberbullying in Schools & the Workplace**, at <http://www.m86security.com/resources/white-papers.asp>.

PROACTIVE REGULATORY COMPLIANCE IN WEB 2.0 LEARNING ENVIRONMENTS

One afternoon in the library media center, Bill was working on a research paper that was due at the end of the week. Clicking from website to website, identifying sources to support his topic, he created a list of sites and citations which he decided to email to himself so that he could easily access them from home. Logging into his personal email account, he found a message from his friend Bob with topless photos of another student attached. Bill opened the email, saw the photos, and forwarded the message to two other friends, then closed the email and went back to his research. A few days later, he was called out of class to the office to meet with his parents, the assistant principal, and the technology director. The technology director showed him copies of the email and pictures as well as the log of sites that Bill had visited that afternoon. When Bill's parents tried to brush it off with "boys will be boys," the technology director replied that this behavior is a clear violation of the District's Acceptable Use Policy and the tools described in the Internet Safety Plan were in place to identify these incidents. Bill served a four-day, in-school suspension as a result.

A number of federal regulations pertain to the use of the Internet in education and affect everything from the secure collection and reporting of student information to the safe and appropriate use of Web sites. These regulations include:

- Protecting Children in the 21st Century Act (Title II of the Broadband Data Information Act)
- Children's Internet Protection Act (CIPA)
- Family Educational Rights and Privacy Act (FERPA)

The **Children in the 21st Century Act** is included in Title II of the Broadband Data Information Act and requires that schools and school districts include in their Internet safety policies a plan for educating students about appropriate online behavior, netiquette, Internet privacy, and cyberbullying awareness¹¹. These information literacy skills are often taught through a school's library media program and are defined by American Association of School Librarians and the Partnership for 21st Century Skills^{12,13}. It is critical that students learn how to appropriately use Web 2.0 tools in the educational context, and not just the social environments with which many are already so familiar. In addition, under the Children in the 21st Century Act, schools applying for E-Rate will have to certify on their 486 Form that their AUP or Internet safety policy clearly states that they are "educating minors about appropriate online behavior, including interacting with other individuals on social networking Web sites and in chat rooms and cyberbullying awareness and response."¹⁴

The **Children's Internet Protection Act (CIPA)** was enacted to provide guidance for E-Rate funding, but other funding resources that require CIPA compliance include No Child Left Behind's Enhancing Education through Technology (EETT) program (Title II-D) and most federal grant opportunities. While the introduction of Web 2.0 resources may increase risk, that risk can be mitigated through policy and intervention rather than prohibiting the use of these tools in the classroom. Socially, students compete to see who can collect the most online "friends," though often these are

people whom they have not met and do not know. In their social space, they may share personal information, making them potential targets for fraud or predators. Students and teachers must learn to use these interactive online tools in the educational arena differently than they use them at home. By clearly setting expectations, defining limitations, and implementing measures to oversee interactive Internet use, schools can enjoy the richness that Web 2.0 tools add to the curriculum while minimizing potential risks and meeting CIPA compliance.

The **Family Educational Rights and Privacy Act (FERPA)** guides and restricts access to student information. FERPA allows parent access to student data until the student reaches 18 years of age. It also allows students and parents to request corrections to inaccurate data. In some cases, such as a dispute related to discipline data, parents have the right to request a formal hearing to reach a decision. While schools have the right to release "directory data," including name, address, birthdate, etc., without parental consent, most requests must be accompanied by a release from the parents.¹⁵ In addition to defining the responsibility schools and districts have to protect student data, FERPA also guides schools in determining the types of information that can be released relative to discipline issues, health situations, and the Individual Education Plans (IEPs) of identified special needs students.¹⁶

IMPORTANCE OF ENFORCING YOUR ACCEPTABLE USE POLICY (AUP)

How does the integration of Web 2.0 tools impact your Acceptable Use Policy? Many district and school AUPs were written years ago and have not been updated regularly. Early AUPs addressed the care and use of student computers. As the use of the Internet and electronic mail grew, language may have been added to address school business versus personal use. With the introduction of Web 2.0 tools, the use of mobile personal computing devices, and the circulation of school devices outside school property, the AUP must now address safety, security, privacy, bullying, and criminal activities, whether inadvertent or malicious.

Technology directors fall into two camps with respect to updating their AUPs. In some districts, the AUP is updated on a yearly basis, or more often as needed, to include specific guidelines on new technologies, including cell phones, Bluetooth, and other devices as they are introduced. Other districts prefer to address the behaviors they consider appropriate rather than list the specific technologies that are used. In either case, it is important that the AUP clearly defines what users can and cannot do as well as the consequences of violating these rules. Violations such as cheating, cyberbullying, and sharing inappropriate pictures of students (i.e., child pornography) range from violations of school policy to criminal activity, and must be dealt with as such. It is the responsibility of administrators to ensure that teachers, students, and parents are aware of and understand updates to the AUP.¹⁷

"We have observed otherwise very complete AUP documents not pass the scrutiny of federal audit when CIPA components are closely examined. In some instances, an amendment to the existing AUP might suffice. In other situations it might be best to draft a new standalone document that clearly outlines the specific CIPA requirements head on."¹⁸

Some districts prefer to amend language to their existing AUP or draft a standalone document to address the use of Web 2.0 tools and resources. Regardless, it is critical to have tools, processes, and strategies in place to enforce AUP guidelines. To protect students as intended by CIPA, the district must ensure that they have the necessary resources and administrative support to enforce their AUP policies.

A COMPLETE SOLUTION FOR THE WEB 2.0 CLASSROOM

In educational environments, most IT leaders prefer to use a multi-pronged, blended strategy that includes **blocking**, **filtering**, **monitoring**, and **reporting** to protect and focus end users. Blocking-only strategies have proven impossible to monitor for even the largest organizations. To assume that blocking a finite number of defined sites will protect students from the ever-increasing collection of Web content is unrealistic. Blocking only provides school leaders with information about where students "cannot go". It does not garner information about what Web sites they are exploring or attempting to reach. An aggressive and proactive strategy is the best plan of attack.

Blocking: The blocking process prevents access to URLs that are known to include inappropriate content, spam, or viruses. For example, many districts block email from hotmail.com. When purchasing blocking and filtering services, the most significant component of the system is the library of sites and the coding strategies used to label Web sites. Jim Culbert, the Information Security Analyst within the Technology Division of the Duval County Public Schools, monitors the activities of over 150,000 users to enforce their AUPs for students and staff. M86 Web Filter collects unrecognized sites in real time and then categorizes each site that evening. This is a process that Duval could not realistically maintain with the existing staff.

Filtering: Unlike the blocking strategy that prohibits access to specific URLs addresses based on predefined lists, filtering prohibits access to Web sites based on criteria defined by IT leaders, educators, and administrators. Filtering strategies allow user groups to be defined with unique access privileges. For example, system administrators may have full access with no filtering; principals may have access to all content except for those sites filtered out as adult content; teachers may have access to social networking sites; but students may not. Sophisticated filtering tools can be implemented to allow students to access blogs, wikis, and social networking sites designed specifically for education, while eliminating access to those that present potential risks.

Monitoring and Reporting: The final component of this multi-pronged approach is to use proactive monitoring and reporting tools to see what users are doing online and how often they do it. Individuals attempting to "hack" the system are generally persistent and will go to great lengths to get around the safeguards in place. These attempts can and should be monitored for patterns in type and frequency. IT staff requires real-time monitoring tools and reports that allow them to be proactive by automating the monitoring process and setting alerts/alarms for behaviors that should be investigated further or brought to the attention of school leadership.

For example, Jim Culbert visits a middle or high school each week with M86 reports in hand to confront students who are violating the district AUP. Based on the detailed information in these reports, students can no longer "talk their way out" of an offense. The district has the data it needs to prove intent regarding the offending behaviors to both students and parents. Upon instituting this strategy three years ago, word has spread quickly throughout the district that they are being "watched", and they will get caught if they do not abide by the district AUP.

The Duval School District uses an Internet Review Committee comprised of administrators, teachers, parents, and other appropriate stakeholders to annually review the access levels defined for the district network users and each of the 100+ filtering categories available. In committee they determine which filtering categories should be applied to each access level for Internet users. The IT department then codes and enforces the decisions of the committee. This process has proven valuable in getting buy-in and developing understanding of appropriate Internet access by all stakeholders. These high-level policies regarding the use of the blocking, filtering, monitoring, and reporting tools for enforcement support the district's multi-pronged safety and security approach. This strategy also helps district IT staff demonstrate compliance, mitigate security risks, prevent data loss, and manage bandwidth more effectively.

PROTECTING YOUR DATA AND NETWORK FROM WEB 2.0 SECURITY BREACHES

From the perspective of IT leadership, long gone are the days of merely checking emails, attachments, and Internet downloads from viruses, worms, and Trojan horses. The introduction of Web 2.0 applications, the use of mobile personal computing devices, and the circulation of school devices outside school property requires greater and more complex security measures to protect both data and network integrity. Today's generation of students completely integrate Web 2.0 applications into their personal lives. Cybercriminals have benefited from Web 2.0's popularity. Malicious content on legitimate Web 2.0 sites is difficult to combat, since most users are constantly engaged in the content. It is the challenge of today's educational leaders to determine how we can responsibly and safely bring these interactive technologies into the classroom without risking the organizations' information and network performance.

From the Washington Post, September 2009:

“In early August, attackers used Clampi to swipe the online banking credentials assigned to the **Sand Springs Oklahoma School District**. The thieves then submitted a series of bogus payroll payments, totaling more than \$150,000, to accomplices they had hired throughout the United States. Sand Springs Superintendent Lloyd Snow said the district has since been able to get about half of those transfers reversed, while the district’s bank graciously covered the rest of the loss. Initially, Snow said, suspicion fell on one school computer on which the Clampi Trojan was indeed found. But a forensic investigation later revealed that a large number of other systems on the board’s network also were sickened with Clampi.”¹⁹

From the Kaspersky Security Bulletin 2009 Statistics:

“Cybercriminals have quickly adapted to take advantage of these new opportunities, and have succeeded in creating fully functional, self-populating botnets using compromised web sites. They have also been quick to exploit the possibilities offered by social networks, and the high level of trust between members of social networks. The likelihood that a member of a social network will launch a file or click on a link sent to him/her by a “friend” is approximately 10 times greater than if the file or the link arrives via email. Cybercriminals actively exploit this trust in order to spread malware and spam.”²⁰

To incorporate Web 2.0 resources into daily practice for teaching and learning in a manner that does not compromise data or network security, districts require protection strategies that:

- Enable administrators, teachers, and students to fully benefit from Web 2.0 applications without compromising security or productivity
- Prohibit crimeware and malicious content from entering the district network

A new generation of malware has emerged in a Web 2.0 learning environment, exposing school networks to new attacks that evade traditional signature-based prevention technologies. Losses due to blended threats and dynamic malware are an unfortunate reality. Developing policies and procedures and investing proactively in strategies now can save districts time and resources in the future. By breaking up malware code into small parts, i.e. mutated code, hackers have created a way to defeat the traditional signature-based malware detection and removal solutions. Mutated malware, after passing through undetected by signature-based security, is reassembled to its original destructive form on the unsuspecting user’s computer. To combat this threat, innovative real-time code analysis solutions are now available to evaluate the intent of a Web page. Mutated malware threats can be detected and removed in real time. Schools should consider real-time code analysis technology as part of their total solution.

Preventing leakage of confidential or sensitive information while providing appropriate and restricted access requires a security strategy that includes a multi-layered approach with the following features:

1. **Anti-virus scanning** minimizes latency because it blocks known malware fast.
2. **URL filtering** quickly ensures user productivity by monitoring and managing where users go online.
3. **Real-time code analysis** stops new and dynamic Web-based threats that typically are not detected by the anti-virus or URL filtering methods.

M86 Security’s patented Real-Time Code Analysis technology achieves the highest rate of malicious code prevention, enabling educational institutions to benefit from the latest Web 2.0 technologies and applications in a secure environment. IT leaders can secure and control the way administrators, teachers, and students use Web 2.0 resources without the need to completely block them. Collaborative applications such as blogs, wikis, and Skype can be controlled, monitored, and restricted to uses beneficial to the teaching and learning in the 21st century classroom.

For detailed technical information on network and data protection, please refer to the M86 Security Thought Leadership white paper, **Strengthening Your Defenses: Web Security & Inbound Malware Protection**, at <http://www.m86security.com/resources/white-papers.asp>.

CELT ACKNOWLEDGEMENT

This white paper was developed for M86 Security by the Center for Educational Leadership and Technology (www.celtcorp.com) located in Marlborough, Massachusetts. For nearly two decades, CELT has helped align leadership, learning, and technology in support of improved student achievement, by working collaboratively with educational organizations to support and transform teaching, learning, and administrative processes. CELT’s mission is to help learning organizations attain their vision, mission, and goals by integrating high-quality programs, services, and technology with the organization’s people and processes in a timely, efficient, and cost-effective way. For the past several years, CELT has been a leader in assessing and designing learner-centered, instructionally focused, and affordable decision support/accountability systems that are valid, reliable, and replicable at the student, classroom, school, school district, state, and federal levels. In addition to helping establish data definitions and systems architecture, CELT assists with the alignment of data systems with contemporary research, best practices, proven business processes, and governance policies.

ADDITIONAL RESOURCES

A Parent's Guide to Internet Safety, U.S. Department of Justice Federal Bureau of Investigation - <http://www.fbi.gov/publications/pguide/pguidee.htm>

CIPA Compliance, Children's Internet Protection Act (CIPA) Compliance - <http://www.untangle.com/Schools/cipa>

Cyber Savvy: Supporting Safe and Responsible Internet Use, A Web 2.0 Approach to Internet Safety by Nancy Willard, updated 2/24/2009 - http://www.educationworld.com/a_tech/columnists/willard/willard008.shtml

E-Rate Central, C.I.P.A. Resources - <http://www.e-ratecentral.com/CIPA/>

GetNetWise, Internet Education Foundation - <http://www.getnetwise.org/>

Mobilizing educators, parents, students, and others to combat online social aggression, Center for Safe and Responsible Internet Use - <http://csriu.org/cyberbully>

National Cybersecurity Alliance. (2008). *National 2008 Cyberethics, Cybersafety, Cybeseurity Baseline Study Key Findings*. From www.staysafeonline.org.

Project Interconnect. (2009). Internet Acceptable Use Policy. <http://www.projectinterconnect.org/filters/aup.htm>

CITATIONS

- Children's Internet Protection Act, Consumer & Governmental Affairs Bureau - <http://www.fcc.gov/cgb/consumerfacts/cipa.html>
- Family Educational Rights and Privacy Act (FERPA) - <http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>
- National Cybersecurity Alliance (2010). *The State of K-12 Cyberethics, Cybersafety and Cybersecurity Curriculum in the U.S. Survey*. From www.staysafeonline.org.
- Children's Internet Protection Act, Consumer & Governmental Affairs Bureau - <http://www.fcc.gov/cgb/consumerfacts/cipa.html>
- What is a Flat Classroom™? (2009) - <http://www.flatclassroomproject.org/About>
- How it Feels to Have a Stroke. (2008) - <http://www.youtube.com/watch?v=UyyjU8fzEYU>
- Uncut: South Hadley superintendent on Phoebe Prince bullying case. (2010, April 7). New England Cable News - <http://www.necn.com/04/07/10/Uncut-South-Hadley-superintendent-on-Pho/landing.html?blockID=211605&feedID=4215>
- Boston students call cyberbullying hot line with complaints. (2010, April 2). Boston Globe - http://www.boston.com/news/local/breaking_news/2010/04/boston_students_2.html
- Boston News Examiner. (2010, February 23). Massachusetts bill would ban cyber-bullying of students - <http://www.examiner.com/x-2398-Boston-Top-News-Examiner~y2010m2d23-Massachusetts-bill-would-ban-cyberbullying-of-students>
- North Country Gazette. (2010, March 7). Statistics: Cyberstalking On Increase - http://www.northcountrygazette.org/2010/03/07/cyberstalking_up/
- Federal Trade Commission (FTC). (2008). Broadband Data Improvement Act - <http://www.govtrack.us/congress/billtext.xpd?bill=s110-1492>
- American Association of School Librarians. (2010). Information Literacy Standards For Student Learning - http://www.ala.org/ala/mgrps/divs/aasl/guidelinesandstandards/informationpower/InformationLiteracyStandards_final.pdf
- Partnership for 21st Century Skills. (2010). 21st Century Literacies - <http://www.kn.pacbell.com/wired/21stcent/index.html>
- E-Rate Central. (2010, May 10). E-Rate Central News for the Week - http://www.e-ratecentral.com/archive/News/News2010/weekly_news_2010_0510.asp
- Family Educational Rights and Privacy Act (FERPA) - <http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>
- Wright, P.W.D & Wright, P.D. (2010). Privacy, Confidentiality, Education Records. WrightsLaw - <http://www.wrightslaw.com/info/ferpa.index.htm>
- Scrogan, L. (2010). AUPs in a Web 2.0 World. EdTech™ Focus on K-12 - <http://www.edtechmag.com/k12/issues/august-september-2007/aups-in-a-web-2.0.html>
- Regional Office of Education, LaSalle County, IL. (n.d.). Guidelines for a CIPA Compliant Internet Safety Policy - http://www.roe35.k12.il.us/Downloads/Guidelines_for_CIPA_Compliance.pdf
- Clamping Down on the 'Clampi' Trojan - http://voices.washingtonpost.com/securityfix/2009/09/clamping_down_on_clampi.html
- Kaspersky Security Bulletin 2009. Statistics, 2009 - <http://www.securelist.com/en/analysis?pubid=204792101>

TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations. Simply contact us or visit www.m86security.com/downloads



Corporate Headquarters
828 West Taft Avenue
Orange, CA 92865
United States
Phone: +1 (714) 282-6111
Fax: +1 (714) 282-6116

International Headquarters
Renaissance 2200
Basing View, Basingstoke
Hampshire RG21 4EQ
United Kingdom
Phone: +44 (0) 1256 848 080
Fax: +44 (0) 1256 848 060

Asia-Pacific
Millennium Centre, Bldg C, Level 1
600 Great South Road
Ellerslie, Auckland, 1051
New Zealand
Phone: +64 (0) 9 984 5700
Fax: +64 (0) 9 984 5720

Version 06/23/10