

SpectorSoft Monitoring for CIPA-Approved Safety and Student Success



Today's students are born and bred on technology; they thrive on music downloads, MySpace, YouTube and instant messaging. Savvy teachers know that harnessing — rather than squelching — youthful skills and ravenous hunger for Internet communication can be a learning opportunity. These teachers also know their “wired” students can easily glide beyond control into Internet abuse, potentially leading to financial drain.

Districts have been held liable when offensive or slanderous materials were sent from school computers. One grade-changing incident cost a school in excess of \$10,000 to correct. Another district paid \$2 million to settle a lawsuit alleging that copyrighted programs were

being unlawfully distributed. Much worse are the costs (financial and otherwise) of a lock-down or school closing from an email threat or bomb scare.

Monitoring + Blocking = Protection

Internet filtering as required by the Children's Internet Protection Act (CIPA) provides a measure of safety, but filtering can be out-manuevered and over-stepped — by students and by web sites. In fact, while a few students seek out inappropriate sites, many more are victimized by unwanted pornographic or disturbing images as they innocently pursue information. Students are also victimized by cyberbullying, but you'll never know it happened if the victim doesn't report it. SpectorSoft provides the safest environment by combining monitoring with blocking. It's like adding camera surveillance to your physical campus gates. You see what gets through.

SpectorSoft's unparalleled, award-winning monitoring

- Shows what is happening right now in quick “Top 10” reports
- Sends real-time alerts of inappropriate Internet searches or communication
- Squashes cyber-bullying by capturing every conversation that takes place

In addition, SpectorSoft monitoring software also

- Filters inappropriate web sites at each computer or centrally by policy
- Blocks Chat/IM applications, ports or all unauthorized contacts

Fast Facts

- In a recent study, 93% of schools reported that teachers or other staff members monitored student Internet access, with 57% of schools using monitoring software.
IES National Center for Education Statistics
- Activities such as hacking, downloading music and videos, and copying CDs are federal crimes, punishable by high fines and prison time. Students as young as 13 years old are being tried as adults...
The Socrates Institute, The CyberEthics Project
- In a recent poll, 48% of 47,235 elementary and middle school students did not consider hacking a crime.
Handbook of Juvenile Justice
- An online survey of 1,400 adolescents in 2005 found that 34 percent had experienced cyberbullying and 17 percent had bullied others.
Center for Safe and Responsible Internet Use
- Many web sites rank thousands of anonymous proxy servers and advertise directly to students the ability to instantly bypass school filters and surf any site, such as MySpace, Bebo, and YouTube.
- 64% of youth who have Internet access at home also go online at school. 11% of all online teens say their primary Internet access location is their school.
Pew Internet & American Life Project
- It is important to emphasize that the high rate of unwanted exposure to online pornography occurred despite the use of filtering and blocking software. Filtering and blocking software alone cannot be relied on for a high level of protection against unwanted exposure and other approaches are needed.
Crimes against Children Research Center

continued...

User Stories

“Right now charts are showing me EXACTLY how many hits websites are getting. Today, Google is getting 1,500 page visits. Right now, on the bandwidth chart, I see one user bringing down large amounts of data. It looks like lots of music.”

“Every August and September, all you need to do is make a couple of examples from student behavior, and you’re set for the coming year. The simplest way to describe SpectorSoft’s impact: major reduction of bad stuff happening.”

Robert Haviland, Technology Coordinator,
Hickman County Schools, Tennessee

“As sophisticated as we thought we were, paying attention to viruses and filtering Internet content, we had no idea what was going on within our own walls. Students were using an ‘anti-proxy’ program, bypassing the content filter by bouncing off another server. With SpectorSoft, now we can monitor even that.”

“It’s human nature; you obey the speed limit because you don’t want to get a ticket. It’s a lot easier to fight off temptation when you know there are consequences. SpectorSoft products keep the good kids good.”

Larry Koby, Director of Information Services,
New Castle Community Schools, New Castle, Indiana

“Our Internet Acceptable Use Policy was a challenge to enforce. Kids are kids. They try to get away with what they can. We found a folder with 60-80 songs deep in our file servers. We wouldn’t have found it without SpectorSoft.”

“Classroom productivity has absolutely increased. SpectorSoft is one of the best software buys we’ve made since I’ve been here; probably the best. It’s our invisible set of eyes. I’m still amazed at what SpectorSoft products can do.”

Jell Hunt, Director of Information and Technology &
Todd Kumpula, Technical Support Engineer,
Park Rapids Area School District, Minnesota



1555 Indian River Blvd.
Bldg. B-210
Vero Beach, FL 32960

888.598.2788 sales
772.770.5670 tech support

www.spectorsoft.com

Monitoring Puts Teeth into Policy

SpectorSoft monitoring software puts teeth in your Acceptable Use Policies by giving you the means to correct the wrong behavior of ANYONE using your computers. It’s becoming a legal necessity. Consider the conviction of the teacher in Connecticut, whose computer displayed pornographic popups visible to students. Because the school could not investigate what really happened, a court was able to sentence her to up to 40 years in prison. Schools with SpectorSoft monitoring software installed, like Hickman County Schools in Tennessee, would be prepared to investigate reasons for and origin of such popups. They’ve been able to send students to detention for accessing porn and fire a teacher for shopping the Internet during class — with proof.

- If someone accesses a pornographic site, they know
- If someone downloads a graphic or video, they know
- If an unauthorized application accesses the Internet, they know
- Screen Snapshots of PC activity show them what happens each day, every few minutes
- If anyone violates policy, they know: who, what, when, where and how

Monitoring Protects Your Network

The Family Educational Rights and Privacy Act (FERPA) requires an institution receiving federal funding to protect the confidentiality of student records and personal information. Encryption, firewalls, and password authentication are mandatory, but monitoring will reveal files being copied, printed or transferred even when an authorized person is logged in. A student in Ohio walked off with district-wide personnel information on a small 30 GB storage device from a password protected system. Without investigative tools, the school could not disprove the student’s claim that the information “just appeared.” Students in the Park Rapids Area School District of Minnesota have no such excuses. With SpectorSoft monitoring software installed, file transfers and network connections are transparent. Rampant downloading and copyright infringement activity has been stopped cold. The school knows:

- Who transferred files via FTP, peer-to-peer or other protocols
- When and where documents were printed or copied onto removable devices
- Exactly when and where a password was entered

They have impartial evidence to retrace steps and share with law enforcement, should the need arise.

Monitoring Adds up to Success

SpectorSoft’s unique combination of Internet in-depth monitoring, filtering and alerting can save your district money, ensure acquisition of much-needed federal funding and help your students succeed. Not only will you meet CIPA and FERPA requirements on nearly every point, you’ll be able to (a) assess usage of applications and resources and prevent unnecessary expenditures, (b) watch students work and adjust instruction for maximum efficiency and (c) enable your students to become responsible online citizens, aware of their actions, focusing on real tasks and real learning.