



Lightspeed Systems Helps Schools Get Smart About Network Filtering and Monitoring to Address Improper Online Behavior

New white paper from network security expert focuses on developing clear acceptable use policies, monitoring online behavior, and conducting forensic investigations

BAKERSFIELD, Calif. – Oct. 28, 2009 – Although criminal activity on school networks is rare, the potential for damage to the people and school involved is extremely high. District and school administrators must be prepared for these situations and equipped with the tools to deter inappropriate behavior, monitor and report online activity, and address problems. To help administrators prevent and prepare for possible crises, [Lightspeed Systems Inc.](#), a leader in network security and management software for schools, has released the new white paper, “Forensics: Identifying, Investigating, and Prosecuting Sexual Misconduct in Your School.”

School safety is one of the top concerns for educators, parents and community members. School officials have an obligation to identify and investigate serious, potentially dangerous, policy infractions. Lightspeed Systems’ white paper discusses how to create acceptable use policies that both deter inappropriate behavior and clearly state violations; how to use network activity reports to identify suspicious behavior; and how to collect forensic evidence necessary to suspend, terminate, or even prosecute violators.

Some of the best practices recommended in the white paper are:

- Update the acceptable use policy annually and keep a signed copy on file for every student, teacher and staff member. The document should provide specific examples of acceptable and unacceptable uses, a listing of all technologies to which the policy applies, usage policies, consequences for infringement, and a disclaimer.
- Conduct regular reviews of user activity. Such reviews are critical to maintain the health and appropriate use of the district network, and to enforce acceptable use policies. In less than 15 minutes a week, administrators can generate and review network activity reports through Lightspeed System’s software.

While up-to-date national statistics are unavailable, a compilation of available research in 2004 suggests that almost 10 percent of students are the targets of sexual misconduct by a school employee at some point during their school career. In many cases, sexual predators do not come under suspicion right away, but they may first cross the line with inappropriate behavior such as bringing pornography into the school and conducting improper communications with students. When monitoring network activity, Lightspeed suggests reviewing: traffic to sites that could be inappropriate, suspicious or blocked searches, users using the network for unnecessarily long periods of time, repeated attempts by a user to access unsuitable content, and high volume communications via e-mail or instant messaging between an educator and a student.

If policy violations are suspected, IT staff must follow certain procedures to protect the individuals involved and the district, and to preserve evidence. Concerns should be brought to district administrators to determine the best course of action, and written permission must be obtained from administrators to investigate the situation further. If child pornography is suspected, law enforcement should be notified immediately.

The white paper also outlines the steps for conducting a forensic investigation to review network history, to examine a user's district-owned computer, and to gather non-computer related information such as school surveillance video.

Lightspeed Systems' [Total Traffic Control](#) network security and management software offers a full range of features in a single comprehensive application. Total Traffic Control combines content filtering, mobile filtering, spam management, bandwidth management, antivirus protection, e-mail archiving, desktop and gateway security, and extensive reporting capabilities.

Lightspeed Systems' network reporting tools help school districts identify all Internet traffic moving through a district-owned network. Lightspeed has tested the accuracy of all reports at a forensic level to ensure they provide an accurate accounting of the activity on each computer.

A free webinar on computer forensic investigation that provides administrators with helpful tips and best practices will be available starting in January 2010.

The white paper is available at <http://www.lightspeedsystems.com/resources/Information-Papers.aspx>. For more information, contact Lightspeed Systems at 661-716-7600, or visit www.lightspeedsystems.com.

About Lightspeed Systems

Lightspeed Systems Inc., founded in 2000, develops comprehensive network security and management solutions for the K-12 education market. Lightspeed is committed to helping schools operate their networks effectively and efficiently, so educators can provide a safe online teaching and learning environment. The company's flagship product integrates content filtering, spam management, bandwidth management, antivirus protection, extensive reporting capabilities, email archiving, and mobile filtering into a single application. Lightspeed Systems software is used in more than 1,500 school districts in the United States, United Kingdom and Australia to protect more than 5 million students. For the past two years, Lightspeed Systems has been recognized on the Inc. 5,000 list as one of fastest-growing private companies. For more information, call 661-716-7600, or visit www.lightspeedsystems.com.

###

MEDIA CONTACTS:

- Crystal Cochran, Lightspeed Systems, 661-431-1649, crystal@lightspeedsystems.com
- Kristen Plemon, C. Blohm & Associates, 608-839-9805, kristen@cblohm.com