

Symantec I-Gear™ — Public school district protects students with good investment.

McCracken County Public School District

McCracken County Public School District (www.mccracken.k12.ky.us) has about 6,800 students enrolled at its six elementary, three middle, and three high schools in Paducah, Kentucky—halfway between St. Louis, MO and Nashville, TN. One of the first districts in Kentucky to be recognized by the Southern Association of Colleges and Schools, each school in the district is accredited by the Kentucky Department of Education.

In addition to offering Internet access to students, the schools provide computer training workshops on such topics as the Internet, email virus protection, PowerPoint, Excel, and desktop publishing. Network engineer Ron Ruggles oversees all aspects pertaining to the district's wide area network that connects to the Internet via a robust T-1 line.

The Problem

While the Internet has been hailed as a great resource for students, it has also been a growing cause of concern for educational institutions across the country. Such is the case for this Kentucky school district. Three years ago, it embarked on a large-scale, multi-phase computer rollout, which saw the number of workstations with Internet access grow from 175 to 1,750. Staff were constantly finding students surfing the Net and accessing objectionable sites. According to Ruggles, it wasn't a secret. "Students were obvious about it," he says. "They'd be huddled over a workstation at the far end of the room, laughing." For Ruggles and other school staff, it was hardly a laughing matter. "They were finding everything imaginable," he says referring predominantly to explicit X-rated web sites.

While the schools were required to monitor students very closely in accordance with the district's Acceptable Use Policy, Internet monitoring was a laborious task. In fact, the only system in place involved lab managers and teachers physically watching students during class and cross-checking computer history files and user sign-in records. Even then, there was no guarantee that unacceptable usage could be proven. "It was a lot of detective work," says Ruggles. "The staff was feeling a lot of pressure. We had some concerned parents who did not want their kids to use the Internet because they could get to anything, anytime." With the radical growth of the district's network about to surge, Ruggles says that not only did they know the violations would increase, but their ability to monitor and control the systems would be "next to impossible."

A
SYMANTEC
CORPORATE
SOLUTION

*"All I had to do was
plug it in, turn it on,
and we were in
business. I was truly
impressed."*

Ron Ruggles
Network Engineer
McCracken County Public School District
Paducah, Kentucky

SYMANTEC.

The Solution

Soon thereafter, Ruggles spotted Symantec I-Gear™ Internet content filtering software at a trade show. He thought it might be the antidote he was looking for: an easy-to-maintain enterprise software package that was locally based, locally managed, and didn't need to be installed and maintained on each workstation. He arranged for a free 60-day online product demo and assigned user accounts to some of the teachers who "knew what the students were accessing."

After spending two months trying to access inappropriate web sites, the teacher testers gave I-Gear favorable reviews. From a network administrator's perspective, I-Gear also offered other advantages that went beyond being able to block unsuitable Internet sites. Ruggles says he was more than satisfied with I-Gear's reporting capabilities, as well as the fact that the software was flexible and easy to maintain.

When it came time to make his case to the school board, Ruggles had no doubt that I-Gear was the solution they needed. "I-Gear was more than competitive. From simply a cost standpoint, it came in thousands of dollars cheaper based on cost estimates of other products, not to mention features that were far better than any other." Ruggles was right. "The Board saw I-Gear as a solution to reduce our risk of liability and as a good investment to protect our students from objectionable content on the web," he says.

Within two days of ordering the software, McCracken received it along with a UNIX server which was custom-configured with the school district's IP addresses and DNS numbers. "All I had to do was plug it in, turn it on, and we were in business. I was truly impressed," he says. Now, when students try to access unacceptable, unblocked sites, lab managers don't have to put on their detective caps and gather clues. They need only pull an I-Gear report by user name or workstation and they have "concrete proof" in a matter of minutes. The site is subsequently blocked and the student is disciplined. What's more, any student who attempts to access 10 unauthorized sites over a 15-minute period is automatically locked out by I-Gear—a move that can only be reversed by asking the school's technical coordinator for access. When that happens, the coordinator simply generates that student's report to isolate the URLs in question to determine the severity of the offense.

So far, reaction to I-Gear has been positive, according to Ruggles. "Some students complain, but most have become accustomed to it." Ruggles especially likes I-Gear's patented Dynamic Document Review (DDR), which has the ability to examine the text of web pages in context and make a blocking decision based on the overall content of the page—not just one or two words. He cites *The Adventures of Huckleberry Finn* as a case in point. While Mark Twain's classic book may contain some text which by today's standards are inappropriate given their racial undertones, I-Gear does not block the book, but rather, just the words considered unacceptable. According to Ruggles, I-Gear is much more than a list of blocked sites. It takes Internet filtering to a higher level than many of the other Internet content monitoring software available. Above all, he says, "I-Gear is a good investment in protecting our children and in the enhanced management of our network."

World Headquarters

20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
1 (800) 441-7234
1 (541) 334-6054

World Wide Web site:
<http://www.symantec.com>

Argentina: +54 11 4811 7526
Austria: +43 150 137 5020
Australia(Sydney): +61 2 9850 1000
Australia(Melbourne): +61 3 9864 2624
Belgium: +32 2 713 1700
Brazil: +55 11 5561 0284
Canada: 1 (416) 441-3676
Caribbean/Central America: +305 228 4555
China (Beijing): +86 10 6465 1237
China (Hong Kong): +85 2 2528 6206
Denmark: +45 45 82 70 40
Eastern Europe Sales Office (Munich):
+49 89 9458 3000
Finland: +358 9 61507 465
France: +33 1 41 38 5700
Germany: +49 21 027 45 30
India: +91 22 2828613
Ireland: +35 31 820 5060
Italy: +39 2 69 5521
Japan: +81 3 5457 5300
Korea: +82 2 3420 8600
Luxembourg: +352 29 8479 5020
Malaysia: +603 7054910
Mexico: +52 5 481 2600
New Zealand: +64 9 309 5620
Netherlands: +31 71 535 3111
Norway: +47 22 65 32 60
Poland: +48 22 528 91 00
Russia: +7095 238 3822
Singapore: +65 239 2000
Spain: +34 (9) 1662 4413
Sweden: +46 8 457 34 00
Switzerland: +41 71 626 20 40
South Africa: +27 11 804 4670
Taiwan: +886 2 2739 9168
UK: +44 1628 592 222

Symantec and the Symantec logo are U.S. registered trademarks of Symantec Corporation. I-Gear and Mail-Gear are U.S. registered trademarks of URLabs, a Symantec company. Other brands and products are trademarks of their respective holder/s.
© Copyright 2000 Symantec Corporation. All rights reserved.
Printed in the U.S.A.
04/00 02-71-00037