

# Walking the CyberHalls

By Ken M. Shaurette, CISSP, CISA, CISM



How important has it become in your school to have the ability to monitor student, teacher and administrator activity while using computer systems?

In the past knowing that there were problems brewing in school was as simple as walking the halls to notice students fighting, bullying or simply planning mischief. In today's technology driven world that has dramatically changed. Computers are available to nearly every student, at home as well as in the school library or computer labs. Computers are necessary to prepare our youth for the

real world, which uses computer systems in nearly every aspect of industry, from diagnosing problems in our automobiles to managing our bank accounts.

Students use computers while in school in a variety of ways. They research their term papers, write stories for English, or look up that illness discussed in Health Class. They even use web sites on the internet to translate words for their foreign language class.

With the wide spread availability of computers also comes concerns of misuse even abuse. Schools have created a policy for acceptable use of computer resources. Even legislation, CIPA, the Children's Internet Protection Act, was created in an attempt to encourage schools to prevent student access to "harmful" and "dangerous" resources. How does a school monitor student, teacher and employee cyber activity? There is more to it than just watching access to the Internet. As a Teacher or Principal, have you ever walked past a student on a school computer, and notice that he or she quickly minimizes or closes the window or program they were looking at? What was the student doing to cause this quick action as you approached? How can a school proactively monitor undesirable activities such as child enticement, access to pornography, or simply abuse of the school acceptable use policy? What about students communicating about bombs, or students changing grades using an administrative or teacher password? What about discussions regarding bringing guns to school using email, instant messenger or some other computer based means? How does a school walk these Cyber Halls?

As I noted in the pre-computer days, you could walk the halls to see problem activity and often know when inappropriate activity was occurring. Now that a lot of student activity has moved to the Computer, how do you "walk the CyberHalls?" Is there a way to track activity of inappropriate student cyber behavior in order to support sanctions or capture the illegal activity by a school official (principal, superintendent or teacher) to provide forensic proof to support immediate actions? Actions might be a warning or a termination and could even lead to criminal action. The potential liability associated with letting activities continue without taking action can be

significant. Even beyond the liability, some activities themselves could be disastrous. (bombs, guns, or child pornography)

A company in Lacrosse, Wisconsin called Sergeant Laboratories has created a solution for "Walking the CyberHalls" named Aristotle. Aristotle allows a school to teach appropriate computer use. It frees technicians or school administration from being the "thought police". It provides no more guessing about the usage of lab computers and software. Aristotle can provide notification of planning activities before the bomb threat, track teacher or student email/chat room harassment, even suicide discussions or plans to run away from home. It can do this all with real-time notification. Custom tailored "security events" when triggered, can be routed to the personnel responsible such as: lab monitors, district administration, or technical school coordinators. The comprehensive reporting allows school board members to understand district computer use and demonstrate computer usage costs during budgeting cycles. Aristotle also gives you the ability to see everything that is done on your computers, down to the keystroke. Through the use of custom security events based on key words which you define, you will be alerted when an incident occurs. If you suspect past inappropriate behavior, simply search for keywords or events and you will have the forensic quality data you need at your fingertips thanks to Aristotle's DataVault™.

I'd like to study briefly a couple real life cases where Aristotle helped a school in very powerful ways. The following Case Studies are based on real incidents, but the specific details described have been modified to protect the privacy of the actual event.

Case Study #1: In my first case study there was a car accident in an upper Midwestern State resulting in the death of two young high school students and serious injuries to two others. Let's examine at how Aristotle had a major impact potentially saving a student's life.

Using Aristotle's feature to track use of words and phrases on computer systems, the Technology Coordinator, tracked "kill myself" and "suicide" for a few weeks after the accident. Within a few days Aristotle alerted the Coordinator that two students had used these words and phrases. In one situation Aristotle identified the user account of a student using WordPerfect to update their personal journal with the message; "I really miss my friend Billy, I don't know what I'm going to do, I miss him so much. I think I'd be better off if I just kill myself."

The entry in the journal of the phrase "kill myself" triggered Aristotle's policy created by the Technology Coordinator to automatically alert him on the use of that phrase. It identified who this student was by their personal school login and even identified the computer lab that they were using to write their journal. Immediate intervention was taken to get this student help. That help may have saved this young man's life.

The other alert was the use of the word "suicide" by a young girl on a school library computer. It turned out that her Health Class was studying Teen Suicide and she was in the process of doing research for the class assignment. She was using the Internet to find more information and statistics, her Google Search included the word suicide. No further action was necessary.

Case Study #2: In our second case students were using a form of Instant Messenger to communicate with each other. This was even after System and Network Administrators thought they had Instant Messenger locked down so that it could not be used.

In a communication between two students, one of the students noted, "I'm ready today, I brought in my gun." When this alert occurred on the word "gun", the Technology Coordinator immediately began drilling down on any other recent communications for this student, using the drilldown by user facility to find any other communications.

What was pieced together was a plot between several students to take revenge on several students that had recently picked on them by shooting up the athletic awards case.

Case Study #3: Our third case reveals Aristotle providing a surprise benefit to school administration. A small Midwestern K-12 School District for several weeks had been researching products that could provide a window into their network. They needed a solution that could help them better understand computer utilization in the district and would help them correct recent computer problems and answer questions from the school board regarding use of technology in the district.

Using the simple installation procedures, the Aristotle agent was installed on over 1000 workstations across the district in less than 2 hours. As soon as the agent was deployed the DataVault™ began gathering information on the applications and activities of all computer usage across the district. It didn't take long to identify a normal usage pattern for most systems and begin to build a profile of how the district's computers were getting used.

One of the first things noticed was a lab that was not getting much use, yet teachers were constantly complaining that they did not have sufficient lab space for their classes. After a little research it was found that class sizes were generally 18-20 students and this lab only had 15 computer systems. After adding five workstations to this lab, Teachers again began scheduling classes in this lab.

The value of Aristotle did not end there. A few days passed before abnormal activity was noticed on the principal at the middle school's computer. It appeared that the principal was using several unusual applications. In addition it was noticed that the principal had visited some rather unique web sites and his use of the instant messenger application increased significantly. Alerts were set off access to file transfer and following a few minutes of researching the data gathered by Aristotle it was found that images were being downloaded from an ftp server located outside the United States.

This sudden increase in unusual activity resulted in the need to begin looking a little further only to find that this principal was downloading child pornography images and was using his instant messenger to communicate with other young children. It appeared that he may have been attempting to entice them to meet with him after school. At this point law enforcement was called and evidence turned over to legal authorities. It is believed that the activity was caught early and a major undesirable situation for the school district avoided.

Summary: These cases are but a few examples of the situations that Aristotle has been involved in. From saving lives and preventing school tragedies to helping manage the computing environment and ensure that acceptable use policy is being followed. More and more schools are finding a need to have the ability to track the use of computer systems. This ability can help you answer questions from the community on how the limited budget is being spent and how much educational value is being gained from the proper use of new technology and applications.

If you wish to get more information on Sergeant Laboratories or request a demonstration visit the web site [provecompliance.com](http://provecompliance.com).