

EFFECT OF MONITORING AND SURVEILLANCE ON DETERRING OFF-TASK  
COMPUTER ACTIVITY AMONG HIGH SCHOOL STUDENTS

by

RICHARD ROSEN  
SpectorSoft Corporation  
Vero Beach, Florida

2006

## **Abstract**

As computers become more central to education, educators are seeking ways to enforce Acceptable Use Policy in regard to computer usage. The purpose of this research was to determine how effectively monitoring student computer activity deters off-task activity. Computer monitoring software in this study was used to record activity in a sample of 80 students at Plainfield South High School. Off-task activity was scored before and after notification of being monitored, and scored again after students were disciplined. Results demonstrated that a highly visible detection strategy and vigorous enforcement of Acceptable Use Policy significantly deters unacceptable computer activity and findings revealed that a small number of students account for the majority of off-task activity.

## Table of Contents

LIST OF TABLES .....	III
LIST OF FIGURES .....	III
CHAPTER ONE: INTRODUCTION.....	1
STATEMENT OF PROBLEM.....	2
CHAPTER TWO: LITERATURE REVIEW.....	4
CHAPTER THREE: METHODOLOGY .....	8
HYPOTHESIS .....	8
METHOD.....	8
PARTICIPANTS .....	9
LIMITATIONS .....	10
INSTRUMENT .....	11
PROCEDURE.....	12
MATERIALS .....	13
CHAPTER FOUR: DATA ANALYSIS.....	13
CHAPTER FIVE: DISCUSSION.....	16
POLICY IMPLICATIONS.....	19
SUMMARY .....	20
APPENDICES .....	22
Exhibit A - Student notification of monitoring.....	22
Exhibit B -Incident tally worksheet .....	25
Exhibit C - Keyword Alerts .....	25
LIST OF REFERENCES .....	26

## List of Tables

Table 1: Instrument Validity .....	11
Table 2: Pre- and Post-Announcement Activity .....	14
Table 3: Post-Discipline Activity.....	15
Table 4: Percentage and number of students off-task.....	18

## List of Figures

Figure 1: Pre- and Post-Announcement Activity.....	14
Figure 2: Frequency Distribution of number of students off-task .....	15
Figure 3: Average and Median Differences.....	17

## Chapter One: Introduction

Computers have become central to the integration of technology into the curriculum, however, along with the benefits an array of problems have been discovered that hinder students from learning. This study utilized computer monitoring software to record in detail how students use computers. The primary research question to be answered by this study was to determine to what degree (if any) does monitoring high school student computer use reduce inappropriate activity and improve time on target. In other words, how effective is deterrence, through detection and accountability, in achieving these objectives?

As computer technology becomes more and more integrated into the curriculum, a great deal of computer output is being generated by students. Because of the concern about the appropriateness of computer activity, management tools and methods must be developed to record, review, analyze and document improper computer activity. Filtering software that blocks and monitors Internet usage increases task focus (Jessup & Urbaczewski, 2002). Filtering software is concerned more with blocking than deterrence and does not concern itself with other types of computer based abuse.

Detailed recording and monitoring of all types of computer activity is just beginning to be widely used in K-12 education. Reports from schools currently using monitoring software show great promise for this issue; however, there is little empirical evidence. This study is needed because of the lack of research in this area. This study will be shared with the education community through publication in educational media and discussion with school personnel, hoping to encourage further research and implementation of computer monitoring in the school community.

## Statement of Problem

Integration of computer based technology into the curriculum has substantially increased in the last two decades and is expected to continue its rapid growth. The Internet in particular has expanded learning opportunities exponentially. The web makes available wide ranging research, communication, and collaborative learning previously confined to local resources. As technology and digital media become more central to student work, student originated problems are increasingly diverting substantial staff resources from instructional technology. Schools need to become aware of what is happening on their computers and implement tools and procedures to detect and deter improper and off-task behavior.

Internet access provides students with unprecedented access to a cyber world that carries obstacles to educational objectives, as well as safety and security concerns. Most prominent is accessing websites devoted to a brotherhood of ill tastes: “pornography, gambling, illegal activities, hate, tasteless materials...violence...threatening emails, offensive chats, copyright liabilities” (Ferrer, 2004b, Challenge section, ¶ 1), bullying, hate mongering and foul language. An area of prominent concern is the web community, such as myspace.com and facebook.com. While the web community provides communication forums that can benefit educational objectives, they can also provide a medium for objectionable activities.

While filtering technology to block these websites is widespread (Curry & Haycock, 2001), it is not foolproof, failing to block 25% of objectionable content and improperly blocking 21% of proper content in this study (Hunter, 2000). While filtering technology has improved since these studies, a study by the University of Michigan sums up the inherent inability of filtering software to serve as a panacea to inappropriate web content. Hansen (2003) stated,

“Because of the enormous amount of uncensored, constantly changing information on the Internet, no filter will ever be free from over- or underblocking errors” (heading 3).

Moreover, filtering often fails to identify or prevent inappropriate, illegal, and even dangerous activity. These include threats to school and staff, hacking into the school network, cyber-bullying and sexual or racial harassment. Teachers, administrators and information technology staff describe other issues they are grappling with (author interviews and communications) as follows:

- Improper discussions in chat rooms, Instant Messaging and blogs.
- Student caused computer and network problems, such as going to websites from which malware and viruses are downloaded.
- Bypassing Internet filters to access websites through proxy servers.
- Use of web mail to bypass school email systems.
- Tying up bandwidth with Internet radio and file downloads.
- Tampering with one’s own or another student's files.

Gebhart (2006) describes the unexpected results when comprehensive monitoring was initiated.

Despite thinking we had a very secure network with high level filtering and policies and procedures in place to ensure staff had students appropriately engaged on computers we still observed many surprising issues. This is what we discovered:

- About 30% of students playing games which are hidden from teachers views as they walk past
- Two students who had staff passwords and have used these to have unrestricted access to parts of the Internet and more

- Several students who have managed to use a bypass proxy web site to access MSN Messenger and run it in the school or configure remote desktop
- Two students who have brought significant hard core pornography into the school on memory sticks
- A number of students who have found websites with pornography that were not blocked by the Department of Education's filter list
- One student using a vampire chat site, indicating that she is in love with an unknown male in the USA and desperate to get a web cam and microphone so that she can chat about her moving to the USA. (possible paedophile)
- Several students using a chat site to discuss suicide
- Regular search by junior students in Google for keywords such as sex, porn etc.
- Cyberbullying (reported to law enforcement)
- Selling of illegal goods on eBay (reported to law enforcement)

Many of our staff were shocked to see what was really happening; however, I believe this is indicative of many high schools in Australia and internationally” (Observations section, ¶ 2).

Filtering takes place at the server while a number of the activities just mentioned can be captured in detail only at the workstation. This research deals with monitoring beyond a filter provided log of websites by elaborately detailing workstation activity.

## Chapter Two: Literature Review

The Internet has expanded communication in business and government<sup>1</sup>, internally and externally. Widespread use of the Internet has created new ways of doing business and improved collaboration and productivity. Internet connectivity has also brought with it an increase in non-work related activities such as game playing, shopping, personnel correspondence and so on.

---

<sup>1</sup> More research has been done on monitoring in business than has been done in education. Because similar problems exist in both areas, research specific to industry generally applies to education.

Acceptable Use Policies were created to counter this misuse, but enforcement has ranged from the extremes of continuous monitoring to none (Jessup & Urbaczewski, 2002). As an example of monitoring (Heuchert, 2005) only when there is probable cause, the University of Virginia prefers "...to encourage people to do the right thing, rather than catching them doing the wrong thing..." (§ 9).

Raul (2006) revealed one reason for detection strategies not being a standard part of an organization's computer policy is the lack of a "prevailing sense of rampant abuses" (slide 2). The pervasiveness of off-task and inappropriate activity is not recognized. For example, the management of a one hundred employee medical company refused to believe their employees' off-task computer activity was a problem, although the information technology staff saw employees taking three hours to do a one hour job, downloading copyrighted music and choking bandwidth. After monitoring was installed, Anderson (as cited in Forrer, 2004a) stated:

When I brought the information to them, they couldn't believe it was happening. They didn't think their employees were capable of the type of activities that were going on. Once I showed them the proof they said 'this is incredible.' It really opened their eyes (Discoveries section, § 2).

Reasons for lack of systematic detection strategies are summarized from an inspector general report on the U.S. Department of the Interior.

...(the) Interior's bureaus either resisted or showed indifference toward participation in the development of criteria for blocking inappropriate sites....there was fairly widespread belief among the bureaus that Internet abuse was not a significant problem...."Absent hard data, the CIOs mostly felt that this wasn't a big deal and didn't merit spending limited resources" (Sternstein, 2006, § 12-14).

Straub and Nance (1990) categorized three major ways of detecting computer abuse: accidental discovery, ordinary system controls, and determined detection efforts. Monitoring software falls into the last category. Straub and Nance found (1990) that without such

determined efforts, discovery usually occurs when an activity triggers an alert or misuse is stumbled upon.

Detection has traditionally focused on system intrusion attacks from outside the organization (Hulme, 2003) while threats originating from within the organization remained under the radar screen. When problems did surface, responses varied significantly from severe discipline to turning a blind eye. In general, accountability and consequences were lax and therefore failed to serve as a deterrent. Hulme (2003) felt:

Because it's so difficult to design, implement, and enforce information-security polices, many companies don't create them. Or they're written and ignored until security problems crop up¶ 4).

However, this is changing. According to Forrester Research, “The digital investigations market is entering its adolescent growth spurt” (Gavin, 2006, ¶ 1). This is spurred by government legislation requiring companies to safeguard personal information and prevent leakage (Wakefield, 2006).

Business is substantially increasing the use of systematic monitoring. The 2005 Electronic Monitoring & Surveillance Survey from the American Management Association found that “Computer monitoring takes various forms, with 36% of employers tracking content, keystrokes and time spent at the keyboard. Another 50% store and review employees' computer files. Companies also keep an eye on e-mail, with 55% retaining and reviewing messages.” (American Management Association, 2005, ¶ 3).

In contrast to these findings, the author, through personal communications with several hundred school IT administrators (2001-2006), found that schools have not similarly increased active, purposeful surveillance of student activity, still relying mainly on filtering software. Schools frequently consider comprehensive workstation monitoring as a reaction to a specific

problem rather than as a proactive policy to deter abuse. As an example, the Highland School of Technology in North Carolina had a serious problem of a server regularly crashing. They suspected student involvement. They installed monitoring software on student computers and discovered students were placing files on network servers. It identified the cause of this problem and the culprit, along with other unexpected network activity and perpetrators (Frost, R. personal communication, Feb. 11, 2003).

In a study of the deterrent effect of monitoring in education, Jessup & Urbaczewski (2002) used a program to monitor two undergraduate classes for off-task computer behavior, with one class being told about it and the other not. The class that was aware of the treatment spent 43% of their computer time off-task whereas the other class spent 51% of their time off-task. In a second experimental study of graduate students, students were told they were being monitored and there would be consequences for off-task behavior. Jessup & Urbaczewski (2002) did not report significance but showed a trend that those aware of being monitored and threatened with discipline were more task focused than those not aware of being monitored.

Students were only orally told that they were being monitored and were not shown sample reports or reminded at each login. Jessup & Urbaczewski (2002) did not address the deterrent effect of actual discipline (in contrast to threatened discipline) or the effect of graphic notification at each login. Also, subjects were undergraduate and graduate level students. It was expected that High School students, being less mature, would have greater off-task activity and may react differently to monitoring.

The research concluded:

- Computer abuse from within an organization is a major problem, from loss of productivity to threats to the organization itself.

- Methods to deal with insider abuse include a systematic detection procedure that identifies off-task activity and those responsible, and provides evidence for enforcement of Acceptable Use Policy.
- Monitoring activity at the workstation level is a critical part of this security strategy.

## Chapter Three: Methodology

### Hypothesis

This study poses two questions: 1) To what extent does regularly notifying students that their computer activity is being monitored deter off-task activity? 2) To what extent does disciplining offenders reduce off-task activity?

It is predicted that a decrease in off-task activity would take place because students are reminded of the monitoring each time they login. In regard to accountability, it is anticipated that a small number of scofflaws will not be deterred by the threat of detection alone, and that discipline, supported by the evidence of graphic monitoring reports, will not only bring them into compliance with Acceptable Use Policy, but deter others as well.

### Method

The research design is experimental with the same sample group measured before and after the monitoring announcement and subsequent to discipline. This study analyzes the effect of monitoring and discipline on two variables, time off-task and type of off-task activity.

## Participants

A sample of eighty participants was randomly drawn from Plainfield South High School population. The school is part of Plainfield Community Consolidated School District 202, which covers 64 miles, located approximately 30 miles from Chicago. Built in 2002, Plainfield South High School is part of a swiftly growing district, which at the time of this study, served 23,822 students from 24 schools (*Our District*, n.d.).

Plainfield South High School has 2,805 students in grades 9-12, ethnically and economically diverse, reflecting the underlying community. Seventy percent of the students come from the city of Plainfield and Joliet (*History and Tradition*, n.d.). Racial makeup of students in 2005 was 77% white, 8% black, 16% Hispanic, and 3% Asian. The "low income" rate is 5.3% for the district compared to 40% statewide. Students meeting or exceeding the standards of the Prairie State Achievement Examination (PSAE) for reading, mathematics and science was 48% in 2004-2005 (*Illinois School Report Card*, 2005).

There were 1,357 students who were not included in the population from which a sample was drawn because they did not use a computer on a regular basis.<sup>2</sup> From the remaining students, a sample of 80 students was drawn using a computer-generated set of random digits. Scoring was self-referenced, with computer activity scored before and after students were made aware of being monitored.

---

<sup>2</sup> Students were eliminated from the sample who did not access the Internet at least one-half hour during the initial two week period of monitoring. Internet use was selected as the criterion because Instant Message, email, game playing, those areas most susceptible to misuse, must have access to the Internet. Of a total of 2,027 logins, 1,448 used the internet for at least one-half hour during the initial monitoring period of two weeks. The sample was drawn from this number.

All student accessible computers (approximately 590) had computer monitoring software installed<sup>3</sup>. Activity was tracked based on user login so a student's activity at any computer in the school could be reviewed.

### Limitations

The variance in time each student uses the computer can affect results<sup>4</sup>. Students included in the sample who used the computer relatively less may not have opportunity to perform off-task behavior as much as students on the computer more frequently. It would be better to have a sample with all students more or less using the computer an equal amount of time. Ideally, a study at a school where all students have laptops or tablet PCs would ensure more equal computer use among students.

Computers were locked out of certain applications, such as email and instant messaging. Therefore, misuse and deterrence could not be measured for these applications. Essentially, only the Internet was available. A study in which as little as possible is restricted would better gauge off-task activity.

---

<sup>3</sup> Computers were not monitored in music, industrial tech and CAD labs for which computers vendors are responsible.

<sup>4</sup> Students who rarely used the computer were eliminated from the population. There were 1931 student logins from the beginning of the spring semester January 3, 2006 to January 31st. However, 483 did not login since January 22nd, most likely because their curriculum does not use computers on a regular basis. It was important to include students in the sample who regularly use a computer. Therefore, these 483 students were eliminated from the population from which the sample was drawn. The remaining population of 1448, from which the sample was drawn, uses the computer in labs at least one hour per week, with most using the computer several hours each week, including use at the library and other locations.

## Instrument

A survey was developed by the researcher with a checklist of inappropriate behavior. Behaviors were drawn from reported experiences of schools currently monitoring computer activity. For each incident, the time was entered into one of the following categories<sup>5</sup>:

- Inappropriate websites visited
- Game playing
- Email
- Foul language and off-task words (See Exhibit C)

A total of the number of incidents was recorded.

Validity was determined by the following correlations, which had to be greater than .2175 to be significant.

pre- and post-announcement	0.2063
pre- and post-discipline	0.3019
post-announce and post-discipline	0.3905

**Table 1: Instrument Validity**

Off-task behavior was scored by first reviewing web site activity. Suspicious activity was crosschecked with program usage to see if there was an educational objective. For example, most searches for autos were off-task. However, some students inserted automotive photos and information into a PowerPoint for a class project and is therefore considered to be on-task. A running total of each type of off-task activity was entered into the instrument.

---

<sup>5</sup> Instant messaging and email applications were not available on school computers. However, such communication was available through Web based blogs, chat rooms and instant messaging. This type of communication was included with general off-task website activity because of the difficulty of isolating it.

## Procedure

Computer monitoring began without student or staff awareness, except for those administrators who needed to be aware of the project. This was important because leaking such information might inadvertently cause deterrence before it was publicly announced. Each student had signed an Acceptable Use Policy when they entered high school, not just prior to the study, so it did not serve as an immediate deterrent. The policy states that computer activity may be monitored and they do not have a right to privacy.

Recording a baseline of off-task incidents and time<sup>6</sup> served as the basis against which the change in off-task activity was measured. After the baseline period of two weeks (period one) ended, all students were notified, through a login notice, that they were being monitored. They were shown samples of monitoring reports and told that their computer activity is being recorded and reviewed (see Exhibit A).

Immediately after the school population was informed that they are being monitored, period two recording began. Off-task activity was again scored. There was an equal amount of time for pre- and post-announcement reporting (periods one and two).

At the end of the reporting period, data was analyzed. The effectiveness of deterrence was measured by the change in time off-task. Results were interpreted and conclusions drawn.

After period two reporting was complete, those undeterred by the monitoring announcement (scofflaws that were drawn from the whole school population) were shown graphic reports of their misbehavior and disciplined. Subsequent to disciplining of scofflaws, it

---

<sup>6</sup> Discerning activities that were off-task is subjective and was occasionally difficult. The student received the benefit of the doubt if it seemed plausible there was an educational objective. Suspect Internet activity was cross checked with program usage to see if it was part of an assignment. For example, a student spent several days on fashion design websites and used the information in a PowerPoint presentation for a class assignment.

was predicted that word-of-mouth would further reduce off-task activity. Two weeks were allowed for word-of-mouth to spread the message that those who violate Acceptable Use Policy will be found. Off-task activity was again scored during period three, the same in length as periods one and two.

Keyword alerts (See Exhibit C) of foul language and off-task words found in e-mail, instant messages and typing were recorded pre-and post-announcement and after students were disciplined. It was predicted that the use of inappropriate language would decrease.

### Materials

Spector 360 software from SpectorSoft Corporation, Vero Beach, Florida, was used to monitor student activity.

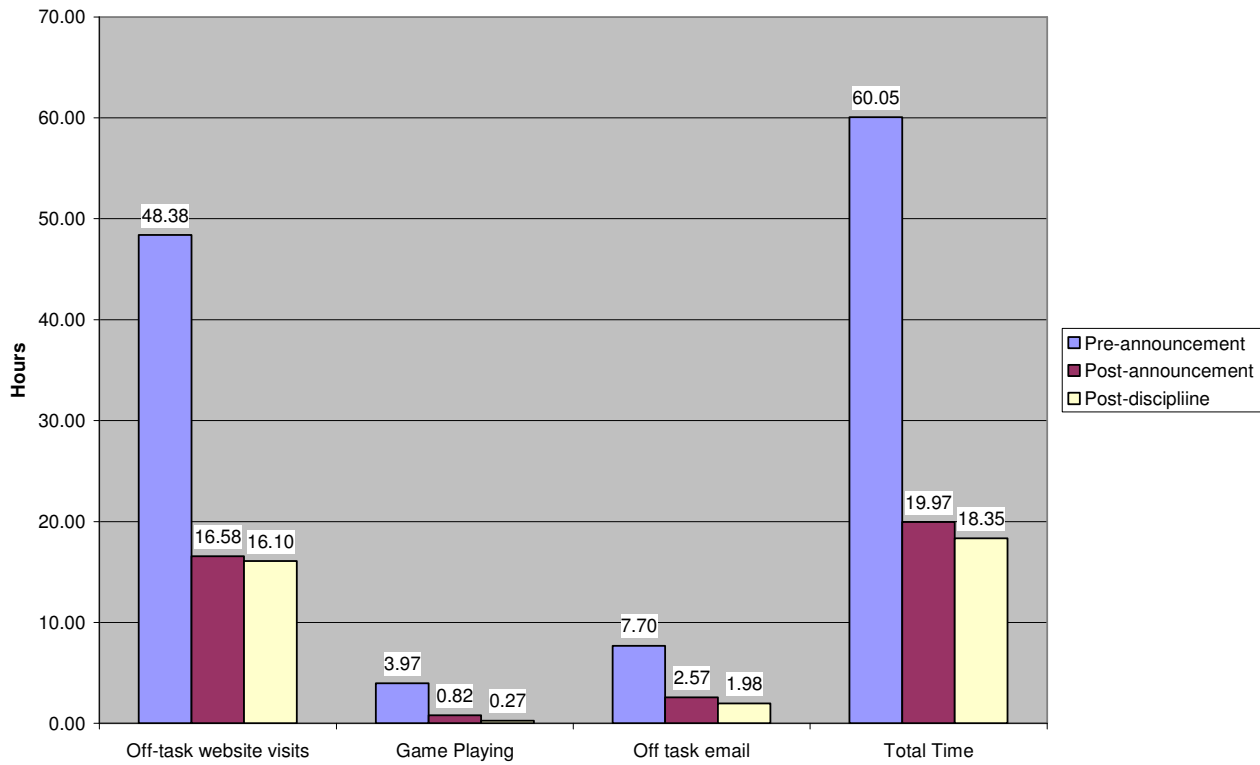
## Chapter Four: Data Analysis

There was a decline in off-task activity of 66.75% in the two-week period after students viewed the monitoring announcement during each login. Median post-announcement off-task activity declined 71%. After scofflaws had been disciplined there was a further average decline of 8.10% and a total median decline of 94% compared to the post-announcement level, indicating a small number of students accounted for the majority of time off-task. (Blocking of websites<sup>7</sup> lessens the validity of this statistic.) Declines in off-task activity were consistent for each type of activity measured.

---

<sup>7</sup> Review of off-task website activity discovered approximately a dozen websites that the school's Internet filtering software failed to block. These sites were then blocked.

**Pre- and post-Announcement Activity**



**Figure 1: Comparison of activity in relation to student awareness of being monitored**

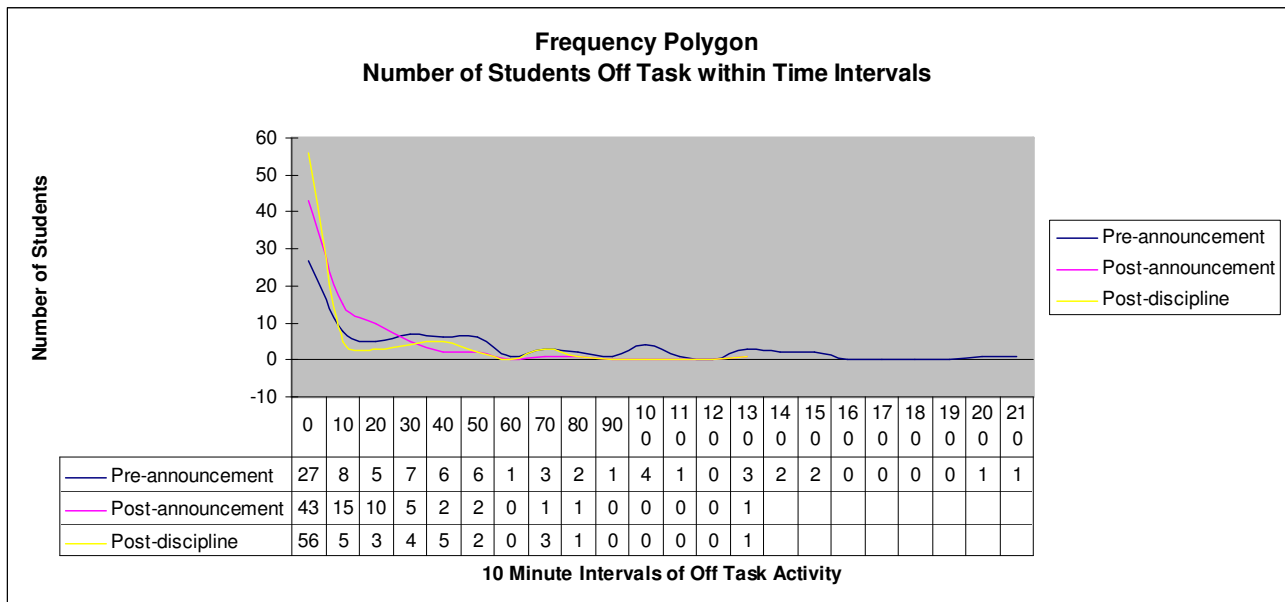
Activity	Pre-Announcement	Post-Announcement	Comparison of Pre- and Post-Announcement	
	Time (hours)	Time (hours)	Time +/- (hours)	Difference
Off-task web site visits <sup>8</sup>	48.38	16.58	-31.80	-65.73%
Game Playing	3.97	0.82	-3.15	-79.41%
Off-task email	7.70	2.57	-5.13	-66.67%
<b>Total Time</b>	<b>60.05</b>	<b>19.97</b>	<b>-40.08</b>	<b>-66.75%</b>

**Table 2: Comparison of activity before and after monitoring announcement**

<sup>8</sup> Website activity includes communications through blogs and web-based instant messaging. From general observation, off-task Web surfing primarily dealt with travel, sports, tattoos, music and cars.

Activity	Time (hours)
Off-task web site visits	16.10
Game Playing	0.27
Off-task email	1.98
<b>Total Time</b>	<b>18.35</b>
-8.10% less off-task activity compared to post-announcement period	

**Table 3: Activity occurring after students were disciplined**



**Figure 2: Frequency Distribution of number of students off-task**

Keyword alerts of foul language and off-task words (See Exhibit C) of the entire school population declined 50.53% subsequent to the monitoring announcement. They declined a

further 6.38% after students were disciplined. In total, alerts declined 53.68%<sup>9</sup> from before the monitoring announcement to after students were disciplined and word spread.

The off-task activity of 19<sup>10</sup> scofflaws declined 91% after they were brought into the assistant principal's office, shown graphic examples of their activity and disciplined.

## Chapter Five: Discussion

The results of the study support the original hypothesis that regularly notifying students that their computer activity is monitored reduces off-task activity and disciplining offenders further reduces off-task activity. Off-task activity declined 66.75% after the monitoring announcement and 69.44% after discipline that resulted in students spreading the word about being monitored. The keyword alert decline of 58% tracks well with the decline in off-task activity and also supports the hypothesis.

Anecdotal evidence had suggested that off-task activity would significantly decrease when students spread the word that their activity is minutely monitored and transgression of Acceptable Use Policy will be punished. Frost reported the following:

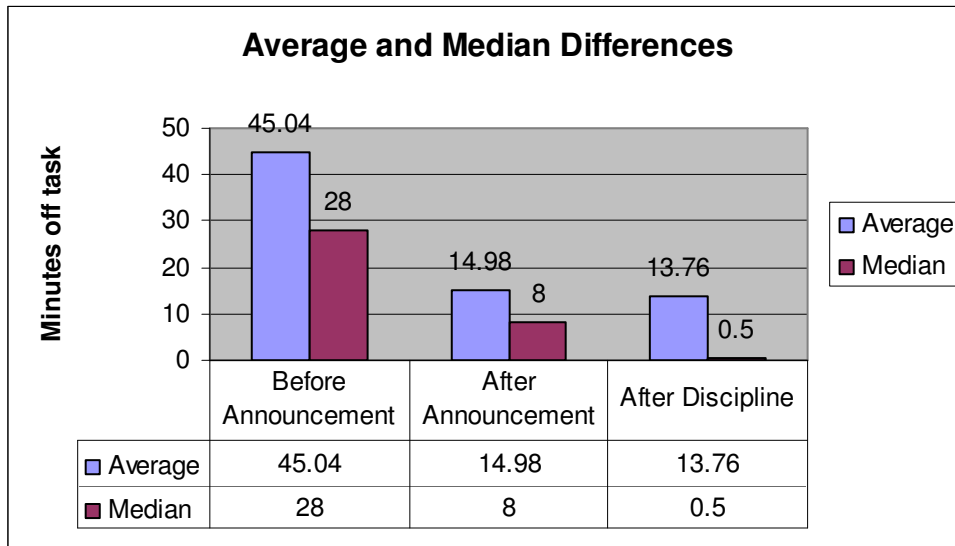
We moved one file onto another computer and called the student in to show it to him. It completely shocked him. "How did you find it?" he asked unbelievably. I replied, "We know a lot more than you think we do; this is just the tip of the iceberg." The word spread like wildfire and it has stopped that kind of behavior cold (2003).

---

<sup>9</sup> Alerts include typed characters and terms found in email and Instant Messages. Web site alerts were significant, but not included because they do not show direct intent to use the terms. Nevertheless, the Web site data is valuable because it indicates Web site activity that may not be appropriate.

<sup>10</sup> There were actually 22 student scofflaws. Three had computer privileges immediately suspended and were dropped from the scofflaw sample.

Additional deterrence resulting from disciplined students telling others is borne out by median off-task activity decreasing from eight minutes post-announcement to 30 seconds post-discipline.



**Figure 3: Average and Median Differences in relation to student awareness of being monitored**

The difference is actually not as great as reported. There would have been more off-task activity had not approximately a dozen websites discovered during monitoring been blocked during this period. Nonetheless, its magnitude suggests the effectiveness of disciplining a small number of students in deterring off-task activity of the general population. While deterrence through word of mouth is outside monitoring technology, it is the information gathered by monitoring that begins the process that ends in word being spread that off-task activity is likely to be detected.

Deterrence has its limits. Some students will risk being detected, as evidenced by four students off-task between 70-130 minutes after discipline. Therefore, ongoing monitoring and continued discipline is required. This is supported by a company reporting that after several

months, some employees gravitated back to off-task activity and had to be reprimanded again (Dotson, B., personal communication, 2006). A study on the long-term effects of discipline would be of value in this regard. This could include sampling student activity at intervals subsequent to discipline to learn the relationship of deterrence to word of mouth over time and the effect of degree and frequency of discipline and number of students disciplined.

A small percentage of students are responsible for the majority of off-task activity. Fourteen students (18%), of the sample of 80, were responsible for over 50% of off-task activity in each of the monitoring periods. This table shows the percentage off-task activity of all 80 students.

	Percentage and number of students off-task			
	less than 30 minutes		more than 30 minutes	
	Percentage	No. Students	Percentage	No. Students
Pre-announcement	50%	40	50%	40
Post-announcement	85%	68	15%	12
Post-discipline	81%	65	19%	15

**Table 4: Percentage and number of students off-task**

A small number of students being responsible for the majority of off-task activity is also demonstrated by median off-task activity being substantially less than average off-task activity.

A significant number of those disciplined did no schoolwork on the computer, but used it only for non-educational activities, as can be shown with the following example. There were 19 students in the student population (not the sample) who ignored the login warning in a significant manner and were disciplined. Eight (42%) did not log in during the two-week period after discipline, indicating they had no computer based class work. For those students who require

continued monitoring vigilance, Spector 360 software allows for periodic reports to be delivered by email on specific students. This would facilitate ongoing enforcement of Acceptable Use Policy.

Frequent graphic reminders of being monitored are an important element in deterrence. The study by Jessup & Urbaczewski (2002) reported a 19% reduction in off-task activity (compared to 67% in this study). A plausible explanation is that “Students were told and reminded throughout the semester the instructor would watch them carefully....” (p. 82). In this case, they were not shown reports, evidence of the thoroughness of monitoring, which would dispel any notion of bluffing or inefficiencies of over-the-shoulder review. And reminders were periodic rather than at every login.

### Policy Implications

Plainfield South High School has web filtering in place. This is the most widespread method among schools to block access to inappropriate websites. Nevertheless, students in the sample spent 48 hours during the two week period before monitoring was announced accessing websites without educational objectives. Monitoring discovered a dozen websites that filtering failed to block, which were then manually added to the filtering list. Furthermore, filtering often fails to discover other violations of Acceptable Use Policy or threats to students, teachers or school. A combination of filtering and monitoring is more effective than either method alone to control off-task activity.

Integrating technology into the curriculum requires open communication. This means the availability of communication tools such as instant messaging and e-mail. All too frequently, schools deal with unacceptable computer behavior by locking down these essential tools. It is

like erecting castle walls, a moat, and a drawbridge to restrict access -- the equivalent of a dial-up connection, limiting learning of 21st-century skills necessary for successful citizenship in our digital society.

A better solution would be to unlock PCs to take full advantage of various communication mediums. Enabling e-mail, for example, would facilitate collaborative projects and communication among students, teachers and administrative staff. Opening school computers to freely access the Internet will enrich the learning experience. Consistent detection and timely reporting of violations will ensure that students use their computers responsibly.

It is amazing how much more responsible students are when they know that what they are typing might be seen by someone else....This method allows the students to learn to monitor themselves while still being accountable for where they go. This software is what education is all about: Freedom with responsibility (Edwards, 2004).

After all the deterrent measures were enacted, off-task activity was still detected. This raises the question as to what degree should off-task activity be permitted and which activities. It is the author's opinion that limited activity, such as checking personal e-mail, should be tolerated in moderation. It is not different in concept than students passing notes among themselves. Furthermore, it is not practical to entirely eliminate it. While you would like to think that a student's time is 100% dedicated to educational activity, it is unrealistic. Even in the workplace, "water cooler" time is an accepted way to intersperse relief with otherwise relentless work.

### Summary

This study demonstrates that systematic and determined detection of off-task activity reduces misuse. Disciplining offenders further reduces it. Heretofore, it has been difficult to

identify transgressors of Acceptable Use Policy. Monitoring software has developed sufficiently to identify offenders and report irregularities through alerting triggers and user friendly reports that readily red flag misuse. It provides a tool to identify irregularities with relatively minimal time and effort. Yet it is not widely used. It is hoped that this study will jumpstart discussion of monitoring in the schools and lead to further research.

## Appendices

### Exhibit A - Student notification of monitoring



#### NOTICE:

Plainfield School District 202 monitors all student computer activity. This is done to ensure:

- Legal compliance
- Computers are used for school related activity
- Compliance with the Acceptable Use Policy you signed when given your ID.

You have no expectation of privacy when using school computers. If you wouldn't want others to see it, don't do it.

These sample reports give you an idea of the information that is recorded:

## Email Activity: A detailed log of any emails sent or received from a District 202 computer

The screenshot shows the Outlook Express interface. At the top is a menu bar (File, Edit, View, Favorites, Window, Help) and a toolbar with icons for Email, Web Sites, Chat/IM, Keystrokes, Programs, Peer to Peer, and Snapshots. Below the toolbar is a search bar labeled "Search Email:" with "Advanced" and "Delete" buttons.

The main area displays a list of email activity with the following columns: In/Out, Type, Sender, Recipient, Subject, and Date Recorded.

In/Out	Type	Sender	Recipient	Subject	Date Recorded
In	POP	dawg@gate.net	kaelie1@gate.net	Emailing: www.discount-cigarettes-store.com.htm	Mon, Mar 21, 2005 03:31:05 PM
Out	SMTP	kaelie1@gate.net	dawg@gate.net	Re: are we off on Monday?	Mon, Mar 21, 2005 03:27:26 PM
In	POP	dawg@gate.net	kaelie1@gate.net	are we off on Monday?	Mon, Mar 21, 2005 03:26:57 PM
Out	SMTP	kaelie1@gate.net	dawg@gate.net	Re: Help me with problem 11	Mon, Mar 21, 2005 03:26:13 PM
In	POP	dawg@gate.net	kaelie1@gate.net	Help me with problem 11	Mon, Mar 21, 2005 03:25:55 PM
In	POP	dawg@gate.net	kaelie1@gate.net	Emailing: Skinhead forums.htm	Mon, Mar 21, 2005 03:23:35 PM
In	POP	spectest1@aol.com	kaelie1@gate.net	password to teacher's account	Mon, Mar 21, 2005 03:18:01 PM
In	POP	spectest1@aol.com	kaelie1@gate.net	Cheat Sheet	Mon, Mar 21, 2005 03:18:01 PM
In	POP	juliet.mcWilliamsvw@ced.fr	ajaim@gate.net	oxycocccntttin no script neeeded	Mon, Mar 21, 2005 03:01:06 PM
In	POP	spidertest@walk.perfect4lif...	dawg@gate.net	hey	Mon, Mar 21, 2005 03:00:55 PM
In	POP	lzqcb@mail.asheville.com	darren1@gate.net	Check it out	Mon, Mar 21, 2005 03:00:54 PM
In	POP	dacds@rhlschool.every1.net	ddwhit@gate.net	What have you got to lose??? . Is it pretty bad? . . . ambig...	Mon, Mar 21, 2005 03:00:51 PM

Below the list, a box labeled "Email example" is shown. The email content is displayed in a large text area:

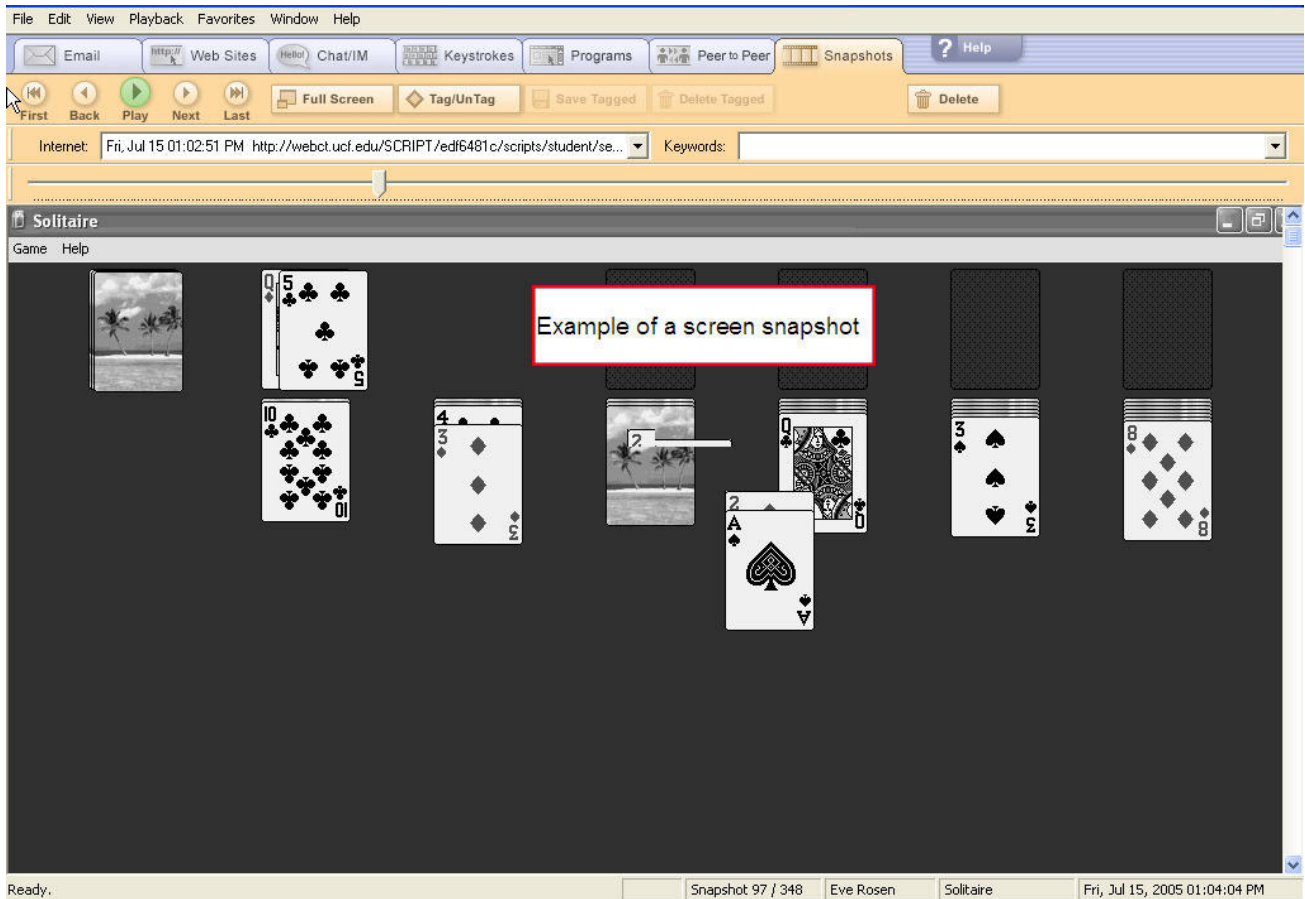
Where were you today dodohead? We are off on monday.

----- Original Message -----  
**From:** [Jenny Monroe](#)  
**To:** [kaelie1@gate.net](mailto:kaelie1@gate.net)  
**Sent:** Monday, March 21, 2005 3:26 PM  
**Subject:** are we off on Monday?

Are we off on Monday?

At the bottom of the window, the status bar shows "Ready.", "Total: 12", "<Unavailable>", "Outlook Express", and "Mon, Mar 21, 2005 03:27:26 PM".

Screen shots: District 202 records VCR like screen shot recordings  
of all activity on the computer



### Exhibit B -Incident tally worksheet

Student Login \_\_\_\_\_

Activity	Running total of time spent
Inappropriate websites visited	
Game playing	
Off-task email	
<b>Total</b>	

### Exhibit C - Keyword Alerts

Pre-Announcement		Post-Announcement		Post-Discipline	
Keyword	Number	Keyword	Number	Keyword	Number
shit	270	shit	126	ass	110
ass	185	ass	96	smoke	102
fuck	153	fuck	83	shit	99
suck	124	nigger	64	fuck	66
damn	124	suck	63	suck	53
bitch	101	damn	47	bitch	44
nigger	96	bitch	47	damn	39
tattoo	40	pussy	15	tattoo	15
asshole	24	fucker	12		<b>528</b>
pussy	23	tattoo	11		
	<b>1,140</b>		<b>564</b>		
		declined	50.53%	declined	6.38%
		compared to pre-announcement		Compared to post-announcement	
				declined	53.68%
				Compared to pre-announcement	

## List of References

American Management Association. (2005). *2005 Electronic monitoring & surveillance survey*.

New York. Retrieved June 10, 2005 from <http://www.amanet.org/research/index.htm>

Curry, A., & Haycock, K. (2001). Filtered or unfiltered? [Electronic version]. *School Library Journal*, 47, (1). Retrieved April 27, 2006, from EBSCOHOST document reproduction service.

Edwards, D. (2004). Maxwell Adventist Academy, Kenya. SpectorSoft Corporation, Vero Beach, FL. Retrieved June 24, 2005 from

[http://www.SpectorSoft.com/products/SpectorPro\\_Windows/customers.html](http://www.SpectorSoft.com/products/SpectorPro_Windows/customers.html)

Forrer, G. (2004a). Medical facility finds key to productivity and savings. Summit Center.

SpectorSoft Corporation. Vero Beach, Florida. Retrieved April 27, 2006 from

<http://spectorcne.com/CaseStudies/SummitCenter.html>

Forrer, G. (2004b). Minnesota school district finds the perfect “classroom monitor.” Park Rapids

Area Schools. SpectorSoft Corporation. Vero Beach, Florida. Retrieved April 27, 2006 from

<http://spectorcne.com/CaseStudies/ParkRapidsAreaSchools.html>

Forrer, G. (2005). Monitoring software helps keep good kids good. New Castle Community Schools. SpectorSoft Corporation. Vero Beach, Florida. Retrieved April 27, 2006 from

<http://spectorcne.com/CaseStudies/NewCastleCommunitySchools.html>

Gavin, M. (With Koetzle, L., Rasmussen, M., & Powell, T). (2006, January 3). CSI: Cyberspace: investigations, evidence, and forensics in the digital world [online], *Forrester Research*.

Abstract. Retrieved April 27, 2006, from

<http://www.forrester.com/Research/Document/Excerpt/0,7211,37400,00.html>

Gebhart, G. (In Press). Creating an Internet Safe School – Real Time Monitoring. *Infonet*. 16, (4) 2006.

Hansen, D. (2003). CIPA: Which filtering software to use? Retrieved April 27, 2006, from

<http://www.webjunction.org/do/DisplayContent?id=992>

Hulme, G.V. (2003, April 14). The threat from inside [Electronic version]. *Information Week*,

Retrieved April 27, 2006, from

<http://www.informationweek.com/story/showArticle.jhtml?articleID=8900062>

Heuchert, D. (2005) Officials warn: Stay away from computer porn. *Inside UVA Online* 35, 7.

Retrieved April 29, 2006, from <http://www.virginia.edu/insideuva/2005/07/porn.html>

*History and Tradition*. (n.d.) Retrieved April 29, 2006, from Plainfield School District web site:

<http://www.learningcommunity202.org/pshs/history.htm>

Hunter, C.D. (2000). Social impacts: Internet filter effectiveness testing: Over- and

underinclusive blocking decisions of four popular web filters [Electronic version]. *Social Science*

*Computer Review*; 18, (2), 214. Retrieved April 27, 2006, from EBSCOHOST document reproduction service.

Jessup, L.M. & Urbaczewski, A. (2002). Does electronic monitoring of employee internet usage work? [Electronic version]. *Communications of the ACM*, 45, 1, 80-83. Retrieved from the ACM Digital Library database.

*Illinois School Report Card*. (2005). Retrieved April 29, 2006, from Plainfield School District web site: <http://www.learningcommunity202.org/Dist202/Report%20cards/2005/phscc.pdf>

*Our District*. (n.d.) Retrieved April 29, 2006, from Plainfield School District web site: <http://www.learningcommunity202.org/Dist202/OurDist/district.htm>

Raul, C.A. (2006) Workplace privacy and employee monitoring, *IAPP National Summit 2006*. Retrieved April 29, 2006, from <http://www.sidley.com/cyberlaw/features/Employee%20privacy-monitoringIAPP3-0906.ppt>

Rosen, R. (2005). Issues of off-task student use. SpectorSoft Corporation. Unpublished raw data.

Sternstein, A. (2006, October 9). Filter catches Interior employees visiting gambling, sex sites. Retrieved October 23, 2006 from <http://www.fcw.com/article96396-10-09-06-Print&newsletter=yes>

Straub, D. W., & Nance, W.D. (1990) Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly*, 14, (1), 44. Retrieved June 30, 2005, from JASTOR COMPLETE Document Reproduction Service.

Wakefield, R.L. (2004, July). Computer monitoring and surveillance. *The CPA Journal*. Retrieved 4.27.06, from <http://www.nyssecpa.org/cpajournal/2004/704/essentials/p52.htm>