THE WEST VIRGINIA PUBLIC EMPLOYEES
GRIEVANCE BOARD

WILLIAM BRYAN HENRY,
Grievant,

v. **DOCKET NO. 2011-0944-DOT**

DIVISION OF HIGHWAYS,
Respondent.

DECISION

This grievance was filed at level three of the grievance procedure by Grievant, William Bryan Henry, on December 31, 2010, challenging a 20-day suspension without pay imposed on him by his employer, Respondent, Division of Highways. The statement of grievance reads:

> I was officially notified in person on December 13th 2010 of receiving a 20 working day suspension of duties without pay starting January 4th 2011 for violating WVOT policy on Information Security and Network Violation Management, specifically by allegedly visiting and attempting to visit numerous known pornographic websites on August 27th, 2010 between the hours of 6:00 am and 2:00 pm. I allegedly was denied access to over 30 requested files that are categorized as known pornography or offensive search engine keywords.
>
> Issue 1: I did not view or attempt to view any pornographic websites as stated. On the date specified I was working an 8 hour shift with a work schedule of 7:30 am to 4:00 pm. These activities began 90 minutes before I ever came to work. The "screen shots" provided were pictures that I have never seen nor requested to see.
>
> Issue 2: A 20 day suspension for a first offence violation of policy is too severe. The information and security policy states that "typically a 15 day suspension is given for first offence." It does not state that more severe penalties are reserved for certain job classifications or degrees of offence.

The relief sought by Grievant is "all disciplinary documents be removed from permanent record stating these allegations. I am requesting reinstatement of (28) twenty-eight days tenure. I am requesting (20) days backpay as well as accrued leave time."

Two days of hearing were held at level three before the undersigned Administrative Law Judge on April 26 and June 10, 2011, at the Grievance Board's Westover, West Virginia office. Grievant was represented by T. Wesley Garrett, and Respondent was represented by Krista D. Black, Attorney, Legal Division. This matter became mature for decision on August 1, 2011, upon receipt of the parties' Proposed Findings of Fact and Conclusions of Law.

Synopsis

Grievant, a supervisor, was suspended for 20 days without pay for accessing and attempting to access pornographic websites on his state computer. Grievant acknowledged that someone had committed this network violation utilizing the identification number assigned to him, but denied that it was he. Grievant's explanation was that he, and others at his worksite, never logged off the computers, and anyone coming into the storeroom to order supplies could access the internet on his computer under his identification number. Respondent demonstrated that Grievant attempted to access a website which is categorized as pornographic by the Office of Technology around 8:00 a.m., on August 27, 2010. Access to this website had been blocked, and access was denied. Respondent did not demonstrate that it was Grievant who accessed and attempted to access pornographic material using Grievant's computer and identification number before Grievant arrived at work, and again later in the day. Grievant demonstrated that the punishment should be mitigated.

The following Findings of Fact are made based upon the record developed at the level three hearing.

Findings of Fact

1. Grievant has been employed by the Division of Highways ("DOH" or "Respondent"), at the District 7 Headquarters in Weston, West Virginia, for seven years. Grievant is a Supervisor 2, supervising three employees in the District 7 storeroom and pipe yard: Eugene Fenster, Brian Stalnaker, and Christopher Harvey.

2. The West Virginia Office of Technology ("OOT") monitors computer usage by state employees in an effort to protect the statewide network from the introduction of viruses and malware which could harm the network. OOT has identified websites which are known to put the network at risk for viruses and malware, or are likely to put the network at risk, and blocks access to these websites. These websites include those considered to be pornographic, websites related to gambling, and those promoting the misuse of weapons. When an employee attempts to access these types of websites, OOT is alerted to the possible network violation, and OOT personnel then review the activity for a period of time to determine whether a violation has occurred. Employees can employ various techniques to defeat the blocked access to websites.

3. The Department of Transportation also has a policy in place which prohibits employees of DOH from accessing "potentially threatening, offensive, or harassing information," including "material that could be construed as . . . obscene, pornographic, profane, sexually oriented or sexually explicit . . . or otherwise inappropriate or illegal." Respondent's Exhibit 21.

4. Prior to August 27, 2010, Grievant had taken the online training course provided by OOT on computer information security, and was aware he was not to access, or attempt to access, pornographic and other non-secure, non-work-related websites. He was also aware of the importance of protecting his password and the importance of logging off the computer when he left his work area.

5. OOT's Information Security Policy states at Section 4.17 that "[e]ach employee must be accountable for securing his or her computer, and for any actions that can be identified to have originated from it." The stated purpose of the Information Security Policy is to establish "objectives and responsibilities for all West Virginia state government agencies, employees, vendors, and business associates, specifically the Executive, regarding information security and the protection of information resources. Respondent's Exhibit 19. (Emphasis in original.) This Policy further provides at Section 5.2.3 that "[e]mployees must guard against access to files and take precautions to protect IT devices when away from the workstation. This includes but may not be limited to the following: Logging off computer . . .."

6. On August 30, 2010, personnel in OOT became aware, during a routine review of activity, that on August 27, 2010, someone had accessed, and attempted to access, pornographic websites on Grievant's computer, utilizing Grievant's identification number, between the hours of 6:00 a.m. and 9:00 a.m., 12:00 p.m. to 2:00 p.m., and after 3:00 p.m. "The computer was denied access to over 30 requests to sites or files that were categorized as known pornography or offensive search engine keywords," as defined by OOT. Respondent's Exhibit 11. The pictures on at least some of these websites were at the very least sexually oriented and sexually explicit.

7. Grievant's work hours in August 2010, were 7:30 a.m. to 4:00 p.m. On August 27, 2010, Grievant arrived at work a little before 7:30 a.m.

8. On August 27, 2010, Mr. Harvey's start time was 6:30 a.m., and Mr. Harvey was at work that day.

9. On August 27, 2010, someone other than Grievant was using Grievant's computer and identification number between 6:25 a.m. and 6:52 a.m. attempting to access what OOT characterized as pornographic websites or using offensive search engine keywords.[1]

10. At 7:27:55 a.m. on August 27, 2010, someone began using Grievant's computer and identification number to conduct a search on the internet. From that time until 7:33:23 a.m., the searches involved various combinations of sal and richard. At 7:46:06 a.m. a new search was begun on Grievant's computer using the internet for "sal the stockbroker," then some miscellaneous non-work-related searches were conducted, and then some "howard stern" searches with various other words included were conducted. These searches continued nearly non-stop until 7:49:41. At 7:54:05 a search was conducted on Grievant's computer, using Grievant's identification number for "raven alexis on sybian." Attempted access to links were denied at this point, as the sites contained

[1] Despite the fact that DOH was aware of Grievant's work hours, that Grievant's computer was accessed almost an hour before his start time, and that Grievant never logged off his computer, no investigation was conducted by DOH to determine who was in the office between 6:25 and 6:52 a.m. using Grievant's computer.

pictures categorized by OOT as pornographic.[2] After this, two "howard stern" and one "sal the stockbroker" searches were again attempted, until 8:00:51 a.m.

11. One of the sites to which the user of Grievant's computer was denied access, and which was flagged by OOT, was related to the search request for "raven alexis."

12. In August of 2010, Grievant had a radio in his office, and every morning Grievant listened to the Howard Stern show on the radio at work, with the volume loud enough that everyone in the office could hear it. Grievant characterized the show as funny, and stated that it sometimes contains sexually-oriented content. Raven Alexis was a guest on the Howard Stern show one morning. She is a porn star.

13. From 13:11:50 p.m. until 13:19:13 p.m. on August 27, 2010, someone used Grievant's computer and Grievant's identification number to conduct internet searches for "vag pics cell phone" and "puss pics." No internet searches had been conducted on Grievant's computer prior to this since 10:41:21 a.m. From 13:19:13 p.m. until 14:00:10 p.m., no internet searches were conducted using Grievant's computer and identification number. From 14:00:10 p.m. to 14:00:24 p.m. an internet search was conducted for "wacker vibratory plate compactor." The next internet search on Grievant's computer using Grievant's identification number began at 15:00:47 p.m. on August 27, 2010, for "aluminum handrail square post brackets."

---

[2] It appears from the testimony of Robert L. Dixon, Manager of OOT's Cyber Security Operations Center, that the user may have been able to view small pornographic images referred to as thumbnail pictures which are part of the Google search results, even though the user could not actually access any of the websites.

14. In August 2010, Grievant, and the three employees he supervised did not log off their computers when they left their work area, and Grievant never logged off at the end of the workday.

15. Grievant's supervisor did not take any action to enforce the requirement that employees log off the computer when they were away from their computers, until after August 27, 2010.

16. No one saw Grievant viewing pornography, or attempting to view pornography, on his computer at any time.

17. DOH employees from all over the District come into the storeroom to obtain supplies throughout the day. As many as 25 people will come to the storeroom on any given day. Grievant's supervisor has witnessed employees other than those who work in the storeroom using the computer of one of the storeroom employees without permission to do so.

18. When OOT personnel were alerted to the fact that someone using Grievant's computer and identification number had accessed and attempted to access websites classified by OOT as pornographic, OOT personnel reviewed the activity on the computer for a 24-hour period surrounding the time period on August 27, 2010. In the course of this review, OOT personnel generated a "Network Violation Report," which summarized the inappropriate searches on August 27, 2010, the times of the searches, search terms, and pictures from websites which had been accessed from Grievant's computer and using Grievant's identification number. The Network Violation Report was provided to DOH.

19. Almost three months later, on November 17, 2010,[3] Grievant was first confronted by DOH personnel with the allegations that he had viewed, or attempted to view, pornography on his computer at work. When Grievant arrived at work on November 17, 2010, he was asked by his supervisor, Melissa Jordan, to meet with her and Peggy Carpenter, District 7 Administrative Services Manager. At this meeting, Grievant was provided with a copy of the Network Violation Report which he had difficulty understanding.

20. Grievant recognized the name Raven Alexis in the search terms found in the Network Violation Report, but he did not recall using his work computer to run this search. He acknowledged that he knew he was not allowed to search for pornographic materials on his computer at work. Grievant believed that had he wanted to run a search for Raven Alexis, it was because he was curious about her appearance, and that he would have used his personal cell phone to run such a search; but, he could not say for certain that he had not run this search on his work computer. Grievant denied that he had used his computer at work to search or attempt to search any of the other websites classified as pornographic by OOT which appear in the Network Violation Report of sites accessed, or attempted to be accessed, using Grievant's computer on August 27, 2010.

21. There is a surveillance camera in the area where Grievant works, which would have shown who was using Grievant's computer on August 27, 2010. The video from the camera is only kept for 30 days, so it was not available by the time Grievant was made aware of the accusations, and no one at DOH had retrieved the video prior to it being destroyed or taped over.

---

[3] It is not clear from the record when DOH was provided with the Network Violation Report, but it appears that the delay was on OOT's end.

22. By letter dated December 7, 2010, Grievant was notified that he was being suspended for 20 working days without pay for "your direct violation of the West Virginia Office of Technology's policies on Information Security and Network Violation Management, and the Department of Transportation's policy regarding Proper Use of Information Technology. More specifically:

On August 27, 2010 during the hours 6:00 a.m. and 2:00 p.m., you visited and attempted to visit numerous known pornographic websites. You were denied access to over 30 requested sites or files that are categorized as known pornography or offensive search engine keywords."

23. Grievant ran various searches for "raven alexis" between 7:54 a.m. and 8:00 a.m. on August 27, 2010, using his work computer. Grievant did not run any of the other inappropriate searches identified in the Network Violation Report on August 27, 2010.

24. Grievant had always received good evaluations, and is considered to be a good employee.

25. Respondent has consistently imposed a 15-day suspension on employees who are not supervisors for a first offense of accessing or attempting to access pornographic websites on a state computer, a 20-day suspension for a first offense if the employee is a supervisor, and dismissal for a second offense.

Discussion

The burden of proof in disciplinary matters rests with the employer, and the employer must meet that burden by proving the charges against an employee by a preponderance of the evidence. *Ramey v. W. Va. Dep't of Health*, Docket No. H-88-005 (Dec. 6, 1988). "The preponderance standard generally requires proof that a reasonable

person would accept as sufficient that a contested fact is more likely true than not." *Leichliter v. W. Va. Dep't of Health and Human Res.*, Docket No. 92-HHR-486 (May 17, 1993). Where the evidence equally supports both sides, the employer has not met its burden. *Id*.

"'As a supervisor, Grievant may be held to a higher standard of conduct, because he is properly expected to set an example for those employees under his supervision, and to enforce the employer's proper rules and regulations, as well as implement the directives of his supervisors.' *Wiley v. W. Va. Div. of Natural Resources, Parks and Recreation*, Docket No. 96-DNR-515 (Mar. 26, 1988)." *Lilly v. Dep't of Transp.*, Docket No. 07-DOH-387 (June 30, 2008).

Respondent clearly demonstrated that someone used Grievant's computer to access, and attempt to access, sexually explicit websites on August 27, 2010. Respondent produced no proof, however, that it was Grievant who did so, and it is clear that it was absolutely not Grievant who was using his computer prior to 7:25 a.m. Despite this evidence, Respondent made no investigation whatsoever into what actually occurred, relying completely on the Network Violation Report.

Grievant testified that he did not remember trying to look up Raven Alexis on his work computer, and did not think he would have, but at one point admitted he could have done so. Grievant's supervisor and Ms. Carpenter both testified that Grievant had admitted to running a search for Raven Alexis when first confronted with the allegations, although Grievant did not remember admitting that he had said he had used his computer at work to conduct this search. As to the remainder of the inappropriate internet searches, Grievant denied that he had accessed or attempted to access the sexually explicit

websites. He readily admitted that he had left his computer unattended, without logging off, thereby allowing access to his computer by other employees in the work area, and anyone coming into the storeroom. In making the determination as to whether it is more likely than not that it was Grievant who accessed the pornographic websites, it is necessary to assess Grievant's credibility.

In situations where the existence or nonexistence of certain material facts hinges on witness credibility, detailed findings of fact and explicit credibility determinations are required. *Jones v. W. Va. Dep't of Health & Human Res.*, Docket No. 96-HHR-371 (Oct. 30, 1996); *Pine v. W. Va. Dep't of Health & Human Res.*, Docket No. 95-HHR-066 (May 12, 1995). An Administrative Law Judge is charged with assessing the credibility of the witnesses. *See Lanehart v. Logan County Bd. of Educ.*, Docket No. 95-23-235 (Dec. 29, 1995); *Perdue v. Dep't of Health and Human Res./Huntington State Hosp.*, Docket No. 93-HHR-050 (Feb. 4, 1993).

The Grievance Board has applied the following factors to assess a witness's testimony: 1) demeanor; 2) opportunity or capacity to perceive and communicate; 3) reputation for honesty; 4) attitude toward the action; and 5) admission of untruthfulness. Additionally, the administrative law judge should consider: 1) the presence or absence of bias, interest, or motive; 2) the consistency of prior statements; 3) the existence or nonexistence of any fact testified to by the witness; and 4) the plausibility of the witness's information. *See Holmes v. Bd. of Directors/W. Va. State College*, Docket No. 99-BOD-216 (Dec. 28, 1999); *Perdue, supra*.

Grievant stated from the first time he was presented with the allegations that, other than the name Raven Alexis, he did not recognize any of the other search terms or websites, and that he would never have used his work computer to look at pornographic websites. He readily admitted that he had not taken steps to secure access to his computer, and that he had taken the training which outlined the importance of doing so. Grievant could not say for certain that he had not searched the name "Raven Alexis" using his work computer, stating that if he had run such a search, he would normally have used his cell phone. This is not surprising given that Grievant was not presented with these allegations for almost three months. It would be difficult for anyone to reconstruct what had occurred in any given workday three months after the fact.

The undersigned finds Grievant to be a credible witness. However, the undersigned must also conclude that, despite Grievant's belief that he would not have engaged in this activity, it is more likely than not that Grievant did run a search for Raven Alexis on his computer at work. The records pulled by OOT for the internet activity on Grievant's computer on August 27, 2010, show that someone was using Grievant's computer nearly continuously to run various searches from 7:27 a.m. to 8:01 a.m. Given that Grievant arrived at work around 7:30 a.m., and was at work that day, the undersigned finds it unlikely that someone other than Grievant would have sat down at his computer for this period of time just as Grievant was arriving at work; and if they had done so, surely Grievant would have seen them.

As to the remaining allegations of inappropriate internet usage, Respondent has not demonstrated that it was Grievant who undertook these actions. It is troubling that Respondent and OOT waited almost three months to take any action in this case. As

Grievant pointed out, he was severely hampered in his defense because the surveillance video was no longer available by the time he or his supervisors were made aware of the allegations. While Respondent and OOT spent a significant amount of time placing evidence in the record about the severity of the risk to the network caused by these types of activities, this testimony is called into question by the delay in response. If the risk is so great, then surely it is imperative that some action be taken immediately to assure that the employee ceases this behavior. It would also seem to be imperative to undertake an investigation to determine who was using the computer to make these searches when it is clear it is not the employee to whom the computer and identification number are assigned, as is specifically the case with the searches which occurred between 6:25 and 6:52 a.m.

The Grievance Board has held that "mitigation of the punishment imposed by an employer is extraordinary relief, and is granted only when there is a showing that a particular disciplinary measure is so clearly disproportionate to the employee's offense that it indicates an abuse of discretion. Considerable deference is afforded the employer's assessment of the seriousness of the employee's conduct and the prospects for rehabilitation." *Overbee v. Dep't of Health and Human Res./Welch Emergency Hosp.*, Docket No. 96-HHR-183 (Oct. 3, 1996). "When considering whether to mitigate the punishment, factors to be considered include the employee's work history and personnel evaluations; whether the penalty is clearly disproportionate to the offense proven; the penalties employed by the employer against other employees guilty of similar offenses; and the clarity with which the employee was advised of prohibitions against the conduct

involved." *Phillips v. Summers County Bd. of Educ.*, Docket No. 93-45-105 (Mar. 31, 1994). *See Austin v. Kanawha County Bd. of Educ.*, Docket No. 97-20-089 (May 5, 1997).

The undersigned must keep in mind that Grievant was a supervisor. In this regard, Grievant did not set a good example by his extensive personal and improper use of his work computer, or by his failure to secure his computer at any time. On the other hand, Respondent's assertions that Grievant's offense was so severe as to warrant a 20-day suspension have been called into question by the delay in response and the failure to conduct a thorough investigation. Grievant was an excellent employee, but Respondent has been consistent in its application of a 20-day suspension for a first offense by a supervisor. Respondent also suggested that Grievant's failure to log off his computer when he left the work area was a more egregious offense than attempting to access a pornographic website. Whether this is true or not, this was certainly a behavior which was easily correctable, but no one ever attempted to correct this behavior until after August 27, 2010. Weighing all the circumstances, the undersigned concludes that Grievant has demonstrated that a 20-day suspension without pay is too severe a penalty in this case. The punishment will be reduced to a 10-day suspension without pay.

The following Conclusions of Law support the Decision reached.

Conclusions of Law

1. The burden of proof in disciplinary matters rests with the employer, and the employer must meet that burden by proving the charges against an employee by a preponderance of the evidence. *Ramey v. W. Va. Dep't of Health*, Docket No. H-88-005 (Dec. 6, 1988).

2. "'As a supervisor, Grievant may be held to a higher standard of conduct, because he is properly expected to set an example for those employees under his supervision, and to enforce the employer's proper rules and regulations, as well as implement the directives of his supervisors.' *Wiley v. W. Va. Div. of Natural Resources, Parks and Recreation*, Docket No. 96-DNR-515 (Mar. 26, 1988)." *Lilly v. Dep't of Transp.*, Docket No. 07-DOH-387 (June 30, 2008).

3. It is improper for state employees to use their work computers to access, or attempt to access, websites classified by the Office of Technology as pornographic, and such attempts place the state network at risk.

4. Respondent proved that Grievant attempted to access a website using his work computer between 7:25 a.m. and 8:00 a.m. on August 27, 2010, which was categorized by the Office of Technology as pornographic.

5. Respondent did not demonstrate that it was Grievant who used Grievant's computer and identification number to access, or attempt to access, pornographic websites at other times on August 27, 2010.

6. The Grievance Board has held that "mitigation of the punishment imposed by an employer is extraordinary relief, and is granted only when there is a showing that a particular disciplinary measure is so clearly disproportionate to the employee's offense that it indicates an abuse of discretion. Considerable deference is afforded the employer's assessment of the seriousness of the employee's conduct and the prospects for rehabilitation." *Overbee v. Dep't of Health and Human Res./Welch Emergency Hosp.*, Docket No. 96-HHR-183 (Oct. 3, 1996).

7. "When considering whether to mitigate the punishment, factors to be considered include the employee's work history and personnel evaluations; whether the penalty is clearly disproportionate to the offense proven; the penalties employed by the employer against other employees guilty of similar offenses; and the clarity with which the employee was advised of prohibitions against the conduct involved." *Phillips v. Summers County Bd. of Educ.*, Docket No. 93-45-105 (Mar. 31, 1994). *See Austin v. Kanawha County Bd. of Educ.*, Docket No. 97-20-089 (May 5, 1997).

8. Grievant demonstrated that the punishment should be mitigated.

Accordingly, this grievance is **GRANTED IN PART, AND DENIED IN PART.** Grievant's 20-day suspension without pay is **ORDERED REDUCED** to a 10-day suspension without pay. Respondent is **ORDERED** to pay Grievant for the 10 additional days he was suspended, and to adjust all leave and other benefits to reflect that the suspension was a 10-day suspension, rather than a 20-day suspension.

Any party or the Division of Personnel may appeal this Decision to the Circuit Court of Kanawha County. Any such appeal must be filed within thirty (30) days of receipt of this Decision. *See* W. VA. CODE § 6C-2-5. Neither the West Virginia Public Employees Grievance Board nor any of its Administrative Law Judges is a party to such appeal and should not be so named. However, the appealing party is required by W. VA. CODE § 29A-5-4(b) to serve a copy of the appeal petition upon the Grievance Board. The appealing party must also provide the Board with the civil action number so that the certified record can be prepared and properly transmitted to the Circuit Court of Kanawha County. *See also* 156 C.S.R. 1 § 6.20 (2008).

BRENDA L. GOULD
Administrative Law Judge

Date: August 31, 2011