



OMBUDSMAN'S REPORT

Complaint Investigation & Findings

OMB04/0121 - November 15, 2004

EXECUTIVE OVERVIEW

The Office of the Community Ombudsman received a call in which the caller (Complainant #1) alleged that a Boise Police officer (Officer #1) had been involved in a sexual relationship with his (Complainant #1's) wife for more than a year. Complainant #1 claimed that Officer #1 had used his position with the Boise Police Department (BPD) to pressure Complainant #1's wife (Complainant #2) into continuing the relationship and had continued to make contact with her, even after she had repeatedly told him (Officer #1) to leave her alone.

The ombudsman's office conducted a thorough investigation into these allegations of possible stalking and telephone harassment. In the course of the investigation, evidence of other potential policy violations came to light. Following the completion of the investigation, the ombudsman issued eleven sustained findings against Officer #1 for violating the following policies (a "sustained" finding means that the preponderance of the evidence proved that a violation of the policy did occur):

- BPD Policy Manual §21.0120 – Unauthorized activities during on-duty time.
- BPD Policy Manual §21.0201 – On-duty behavior likely to bring discredit on the department.
- BPD Policy Manual §24.1300 – Unauthorized personal use of BPD cell phone and failure to reimburse the department for personal use.
- BPD Policy Manual §21.0504 – Failure to comply with computer security requirements.
- BPD Policy Manual §21.0501 – Unauthorized personal use of department computer equipment and software.

- BPD Policy Manual §21.0502 – Use of department internet access to visit pornographic sites; use of department email system to send inappropriate content.
- BPD Policy Manual §21.0317 – Unauthorized sending of confidential department and personnel information via email to persons outside the department.
- BPD Policy Manual §21.0308 – Behavior and statements likely to cause offense and a hostile work environment.
- Boise City Policy Manual §1.04 – Behavior and statements likely to cause offense and a hostile work environment.
- Boise City Policy Manual §7.28 – Use of the services of on-duty department employees to perform tasks related to Officer #1's outside employment (City Code of Ethics and Fiduciary Duty).
- BPD Policy Manual §22.0110 – Making false statements in the course of an official ombudsman investigation.

The ombudsman issued one not sustained finding (a “not sustained” finding means that the preponderance of the evidence neither proved nor disproved that a violation of the policy did occur) in connection with the following allegation:

- BPD Policy Manual §21.0317 – Alleged unauthorized disclosure of a computer security password to Complainant #2.

The ombudsman also issued the following two unfounded findings (an “unfounded” finding means that the preponderance of the evidence proved that a violation of the policy did **NOT** occur):

- BPD Policy Manual §21.0302 – Alleged illegal behavior (stalking and telephone harassment).

BPD Policy Manual §21.0209 – Alleged acceptance of discounts from merchants in violation of department policy.

BPD Policy Manual §21.0202 – Alleged ethics violation for use of official position to obtain discounts from merchants.

In light of what was found during this investigation, the ombudsman also made the following policy and training recommendations to the chief of the Boise Police Department:

Harassment Policy Training

Given what was learned in the course of this investigation, particularly regarding inappropriate and questionable behavior that had been widely known but not directly confronted, BPD supervisors may benefit from additional training regarding their obligations to implement and enforce Boise City's harassment policy. The harassment policy dictates strict requirements for supervisory response to such behavior in order to protect employees from behavior that is, or could become, harassment. This policy is also designed to protect the city and its departments from the liabilities associated with violations of the harassment policy. It is recommended that the department review and improve (if necessary) its training and communication of this important policy area.

Cell Phone Reimbursement

It is recommended that BPD's practice regarding cell phone reimbursement be evaluated. It appears that the current policy requirement regarding reimbursement is not being consistently and strictly enforced. This use of public funds for personal purposes, in the form of un-reimbursed charges for cell phone time over the pre-paid plan, must be discouraged.

Administrative Leave Letters

It is recommended that BPD require its supervisors to use a standard letter when placing employees on administrative leave. When an administrative investigation is underway and it becomes necessary to place an employee on administrative leave, correspondence to the employee should clearly state that he or she is being placed on administrative leave with pay and that this action is non-punitive and non-evaluative. Such correspondence should also clearly state that the affected employee is to have no contact (whether in person, via telephone, by email, or in any other form) with department employees other than a designated contact (generally the direct supervisor). It is also recommended that, while an employee is on administrative leave, access should be blocked to City email, all other Boise City computer systems, and all City facilities without public access.

Email Audit

It is recommended that BPD conduct an immediate audit of email activity by and among its employees. Certain content, such as that found in the course of this investigation, can be a violation of email and harassment policies. Our review of only one email account (that of Officer #1) indicates that the sending and receipt of inappropriate emails in BPD was not limited to that one individual.

Internet Access

This investigation revealed that a significant number of computer users at BPD have unrestricted and unmonitored access to the internet. It is recommended that BPD review the advisability and necessity of unrestricted internet access by any BPD employee. While legitimate investigative and department business may necessitate the granting of such access, this should be done on an extremely limited basis. Furthermore, it is recommended that BPD institute a policy and practice of regularly auditing any computer accounts granted unlimited

internet access. Doing this will help ensure that the viewing of pornographic or otherwise objectionable material is strictly limited to instances where legitimate police business requires it.

THE COMPLAINT

On July 6, 2004, The Office of the Community Ombudsman received a call in which the caller (Complainant #1) alleged that a Boise Police officer (Officer #1) had been involved in a sexual relationship with his (Complainant #1's) wife for more than a year. Complainant #1 claimed that Officer #1 had used his position with the Boise Police Department (BPD) to pressure Complainant #1's wife (Complainant #2) into continuing the relationship and had continued to make contact with her, even after she repeatedly told him (Officer #1) to leave her alone.

Complainant #2 further alleged that:

1. Officer #1 routinely used a BPD cell phone to call her during the day, including instances in which she and Officer #1 had conversations of a graphic sexual nature.
2. Officer #1 and Complainant #2 had sexual contact while Officer #1 was on duty, including numerous occasions when he came home from work in the middle of the day and one time when the two of them spent two to three hours in a hotel room while Officer #1 was thought to be working a night shift.
3. Officer #1 gave rides to Complainant #2 in his assigned BPD vehicle, including one occasion when they drove to an area on Highway 21 past the Hilltop Café so Officer #1 could view Complainant #2's underwear.
4. Officer #1 revealed to Complainant #2 the password to the mobile data terminal in the police vehicle assigned to Officer #1.
5. Officer #1 had received sizable discounts from two local hotels and one car dealer.

In the course of investigating the allegations made by the complainants, evidence of the following additional policy violations came to light:

1. Alleged failure by Officer #1 to reimburse BPD for personal use of a cell phone owned by BPD.
2. Alleged use by Officer #1 of other BPD employees (while they were on duty) to perform tasks related solely to Officer #1's outside, private employment.
3. Alleged failure by Officer #1 to follow department security policy and log off his computer when leaving it unattended.
4. Alleged unauthorized email sharing of confidential police and personnel information with persons not employed by BPD.
5. Alleged unauthorized personal use of BPD computer equipment and software.
6. Alleged unauthorized use of BPD computer and internet access to view pornographic material.
7. Alleged harassment of other BPD employees through comments, remarks, and sending offensive and/or degrading email.
8. Alleged false statements to the assistant community ombudsman while answering questions in an official investigation.

THE COMPLAINT INVESTIGATION

Given the allegation that Officer #1 had engaged in behavior that might be a violation of Idaho Code §18-7905 (Stalking) and §18-6710 (Telephone Harassment), the ombudsman first sought an opinion from the prosecutor (Boise City Prosecutor) who would have jurisdiction to bring charges if the evidence warranted. The Boise City Prosecutor sent the case to the Canyon County Prosecuting Attorney due to the potential for a conflict of interest. After a review of the allegations made by Complainant #1 and Complainant #2, the Canyon County Prosecuting Attorney declined to open a criminal investigation due to insufficient

evidence to believe that a crime had occurred.

The assistant community ombudsman was assigned to conduct the investigation of the allegations made by both complaints. In the course of this investigation, 24 individuals were interviewed, including Complaint #1, Complainant #2, Officer #1, 18 other BPD employees, and three witness not employed by the City of Boise. The three non-employee witnesses were local merchants who had reportedly given Officer #1 discounts on goods and services. The investigator also obtained and analyzed BPD personnel records, cell phone bills, and reimbursement records.

In addition, the services of three computer experts employed by the City of Boise were used. One of these experts conducted a forensic exam of the hard drive on the BPD computer that had been assigned to Officer #1. The other two computer experts provided the investigator with complete lists of all internet activity by Officer #1 between February 2, 2004, and July 29, 2004, as well as access to past email messages sent to and received by Officer #1 through the City's email system.

At the conclusion of the investigation, the ombudsman determined that there was sufficient evidence to form a reasonable suspicion that Officer #1 may have violated Idaho Code §18-5701 (misuse of public money by officers) in that he made personal and unauthorized use of a BPD cell phone and failed to reimburse the City of Boise for the specific overtime charges (\$331.51) associated with that use. The ombudsman consulted with the Boise City Attorney's Office and, because the potential violation was a felony, the matter was referred to the Office of the Ada County Prosecutor. The ombudsman provided the Ada County Prosecutor's Office with the evidence (excluding any information or evidence obtained as a result of statements made by Officer #1 in a compelled interview) and asked for a determination. The matter was conflicted out to the Canyon County Prosecuting Attorney.

WHAT THE COMPLAINT INVESTIGATION FOUND

Alleged Stalking And Telephone Harassment

Interviews of Complainant #2 and Officer #1 clearly showed that the relationship between them had been mutual and consensual. The relationship had begun as acquaintances and transitioned into something more intimate sometime in the second half of 2002 or early 2003. While it is true that Complainant #2 attempted to end the relationship on more than one occasion by telling Officer #1 not to contact her, it is also the case that Officer #1 made similar efforts himself. In the final analysis, both Officer #1 and Complainant #2 permitted and encouraged the relationship (on an on-again, off-again basis) until it finally ended in the Spring of 2004. In the opinion of the Canyon County Prosecutor and the ombudsman, no act of criminal stalking and/or telephone harassment took place.

Use Of BPD Cell Phone For Other Than Official Business And Failure to Reimburse BPD

The monthly billing records for the BPD cell phone assigned to Officer #1 were audited. This audit covered a 32-month time span from December 26, 2001 through July 16, 2004, during which, according to Complainant #2, she and Officer #1 were engaged in an intimate relationship. The audit revealed that Officer #1 spent a total of 2,132 minutes in outgoing calls placed to either Complainant #2's home phone number or her cell number. Due to the manner in which BPD's cell phone provider documented incoming calls, it was not possible to determine how many of the incoming call minutes on Officer #1's cell phone originated from either of Complainant #2's phone numbers. A review of Complainant #2's cell phone bill for the first six months of 2004 revealed that she placed a total of 21 separate calls (totaling 106 minutes) to either the office or the cell phone numbers assigned to Officer #1.

While no recordings were found of any of these telephone conversations between Officer #1 and Complainant #2, interviews of both parties support the conclusion that some of the calls

were of a sexual nature. No evidence was found to suggest that any of these cell phone calls were related to official BPD business.

A further analysis of the bills for Officer #1's assigned cell phone demonstrated that, for the 32-month period under review, a total of \$379.59 in excess time charges had been paid by BPD for calls made by Officer #1 to Complainant #2. During the same period, Officer #1 reimbursed BPD a total of \$48.08 for personal use of the department cell phone. This left \$331.51 in unauthorized personal cell phone usage for which Officer #1 had not reimbursed to BPD. While Officer #1 had been given a copy of each monthly cell phone bill for the period under review, it must be pointed out that BPD never sent Officer #1 a notice or bill specifically requesting reimbursement for his personal use of the cell phone.

At the conclusion of this investigation, on November 2, 2004, Officer #1 made a payment of \$331.00 to BPD for reimbursement of past personal cell phone use.

Engaging In Non-police Business While On Duty And On-Duty Behavior Likely To Bring Discredit On The Department

The evidence obtained in the investigation shows that, on numerous occasions, Officer #1 engaged in sexual activity with Complainant #2 during periods when he was considered to be at work. This included brief encounters in Officer #1's house during the day, as well as one specific occasion when Officer #1 and Complainant #2 had sexual contact in a hotel during a two or three hour period in the evening while other on-duty BPD officers assumed Officer #1 was out on patrol.

The investigation also found that Officer #1 used a BPD police vehicle to drive Complainant #2 along Highway 21 past the Hilltop Café, but before the High Bridge over Mores Creek. While on this drive, Officer #1 parked the police vehicle and viewed Complainant #2's underwear. During the time that Officer #1 was east of Luck Peak Dam, he was completely

out of range for use of the two-way radio in the police vehicle, his BPD pager, and his cell phone. In other words, Officer #1 could not be reached by BPD or Ada County Dispatch for the 30 to 45 minutes that he and Complainant #2 spent on this trip.

Release Of A Confidential Password To The Complainant

The investigation failed to develop sufficient evidence to either prove or disprove the allegation that Officer #1 gave his mobile data terminal (MDT) password to Complainant #2. In the final analysis, it was his word against hers.

Use Of Official Position To Receive Discounts

Complainant #2 reported that Officer #1 told her he knew lots of merchants in town and, as a result, was able to get substantial discounts at two Boise hotels and a local car dealer. Management staff at both hotels were interviewed. They confirmed that Officer #1 had been given discounts on hotel rooms he booked for himself and for friends. However, both hotel managers insisted that these discounts had nothing to do with Officer #1's position with BPD. They said that he had been given discounts that are available to anyone who is a friend or family member of a hotel employee. One of the hotel managers said that he first got to know Officer #1 some years back when their children were on the same youth sports team together. The other hotel employees said they first met Officer #1 through his police work, and later developed friendships with him that were not connected to his position with BPD.

Regarding the information that Officer #1 may have received a discount from a local car dealer, the information provided by Complainant #2 was not specific enough to warrant further investigation.

Use Of Other BPD Employees to Perform Work Related To Outside Employment

As the investigation into Complainant #2's allegations progressed, several BPD employees who work closely with Officer #1 were interviewed to determine if, in light of the alleged relationship with Complainant #2, Officer #1 had been absent from his work or neglectful of his duties. In the course of these interviews, the investigator was told that Officer #1 had asked one or two other employees to perform tasks that were unrelated to official BPD duties. Both employees were interviewed. They confirmed that, on two separate occasions in the past year, Officer #1 (who supervised them) had asked them to complete computer work on projects related to Officer #1's outside, non-BPD employment. One employee estimated that the task had taken approximately two hours to complete; the other employee said it took about four hours to do the work. It was estimated that the direct labor costs associated with these six hours of lost productivity were less than one hundred dollars. Both employees confirmed that they performed the work while on-duty for BPD and that the tasks were not part of their normal BPD duties. One of the employees provided the ombudsman's office with copies of the work product that was produced by the two employees for Officer #1. A search of the hard drive on the BPD computer assigned to Officer #1 revealed electronic versions of these same documents.

Before proceeding with this line of the investigation and questioning Officer #1 about it, the ombudsman reviewed the allegation with the Boise City Attorney's Office. The assigned assistant city attorney consulted with a prosecutor from the Office of the Idaho Attorney General who is experienced in prosecuting cases related to the misuse of public assets. The ombudsman was informed that, while Officer #1's action may have been a violation of Boise City's Code of Ethics, it did not appear to be a criminal act under Idaho statutes.

Following this legal opinion, Officer #1 was questioned about his use of two BPD employees to perform tasks associated with his outside employment. Officer #1 admitted that he had done this.

Unauthorized Use of BPD Computer Equipment and Internet Access

When the investigator searched the hard drive of Officer #1's BPD computer looking for documents related to Officer #1's outside employment, evidence of pornographic web sites was discovered. The computer was seized as evidence and a forensic examination of the hard drive was conducted. The hard drive contained evidence that 97 different web sites containing sexually explicit photographs and other content had been accessed in 2004 using that computer and Officer #1's password-protected user name. In addition, the hard drive contained evidence of heavy use of the internet to view web pages relating to sports and personal entertainment not related in any obvious way to official BDP activities. The hard drive also contained a digital file that contained a pornographic video. It should be noted that no evidence of child pornography or other unlawful content was found on the computer's hard drive or any of the web sites visited by Officer #1.

The investigator then reviewed the records maintained by Boise City's Information Technology Department of internet access under Officer #1's user name for the first half of 2004. The same web addresses of pornographic web sites appeared in these records, along with other sports and entertainment sites that did not appear to be directly related to Officer #1's police duties.

Officer #1 was asked by the investigator if he had used the BPD computer assigned to him to access pornographic and other unauthorized web sites. He denied intentionally visiting any pornographic sites, but admitted to visiting some sports and non-pornographic entertainment sites. Officer #1 claimed that several other BPD employees (whom he named) knew his user name and password. He speculated that one of them could have visited the pornographic sites under his (Officer #1's) user name. Officer #1 said that several months earlier someone loaded a picture of a naked elderly woman onto his computer and set it as the "screen saver". Officer #1 said he thought this was just a joke. He also said that, on three occasions, he "clicked" on a pop-up advertisement and found the computer displaying a pornographic web

site. Officer #1 denied any knowledge of the pornographic video found stored under his user name on the computer.

All of the individuals named by Officer #1 as persons who knew his user name and password were interviewed. Each knew Officer #1's user name, but denied knowing his password during the time period under review. These witnesses did say that Officer #1 had a habit of leaving his computer powered up and logged onto the network under his user name. The witnesses said that Officer #1 did this intentionally because he wanted other employees to feel welcome to use his computer when he was not there. Some of the witnesses said that they warned Officer #1 that he was making himself vulnerable to pranks and compromising the security of the computer system.

The investigator then looked at records of Officer #1's email activity and electronic calendar entries for the days on which the pornographic web sites had been accessed. These records showed that, on at least two separate occasions, Officer #1 sent emails from his computer on the same day that pornographic web site activity had been documented. The investigator also used BPD payroll records to confirm that Officer #1 was on duty and not on leave or at training on the days when the pornographic web sites were visited.

Officer #1 was re-interviewed and confronted with the evidence that had been gathered in connection with the pornographic web site activity. After being confronted, Officer #1 admitted that he had personally accessed those sites and viewed the pornographic video on the BPD computer assigned to him. Officer #1 said that his initial denial was not true. Officer #1 admitted that he had not been truthful when he told the investigator that others had access to his computer password. He also said that he had been untruthful regarding the story about the pornographic screen saver he said appeared one day on his computer.

Making False Statements In An Ombudsman Investigation

As noted above, Officer #1 initially denied intentionally using a BPD computer and network to access pornography or other objectionable material. In addition to this denial, Officer #1 attempted to deflect suspicion from himself by inventing a story that pornography appeared on his computer one day and telling the investigator that several other BPD employees had access to his computer password. These denials and fabrications caused the investigator to spend considerable time attempting to verify or refute them. Officer #1 also caused suspicion to fall on other employees as a result of his false statements. Officer #1 only admitted the truth of his actions after the investigator confronted him with evidence proving his culpability.

Failure To Follow Required Computer Security Practices

Several of Officer #1's fellow employees reported that he routinely left his computer on and logged into the BPD computer network, even overnight and times when he was gone from his office for several hours. Officer #1 admitted that this had been his practice for some time.

Unauthorized Release Of Confidential Police and Personnel Information

In the course of reviewing Officer #1's email messages for the first half of 2004, the investigator found evidence that Officer #1 had sent emails containing confidential law enforcement and personnel information to someone not authorized to receive it. The confidential information included names of crime victims, medical information about a BPD employee, and possible personnel action to be taken by BPD.

Officer #1 admitted sending the information and confirmed that he had not received authorization to send it to the recipient of his email messages.

Workplace Harassment

As the investigation progressed, employees who worked with Officer #1 told the investigator about comments made in the past by Officer #1 that some employees found objectionable. It must be noted, however, that not all of Officer #1's fellow employees were offended by Officer #1's comments.

The comments reportedly made by Officer #1 included complimenting female employees on their clothing, hair style, physical attributes, and perfume. One female employee reported that Officer #1 did not similarly compliment female employees on their work performance.

One female employee reported that Officer # 1 made a sexually suggestive remark to her that she found very offensive. She reported that she was in a closed-door meeting with a male BPD employee when Officer #1 knocked on the outside of the door and yelled her name saying, "Pull up your pants." This same female employee also reported that Officer #1 had sent her an email containing a picture of a female, whose buttocks were bare, riding on the back of a motorcycle. This employee said she found the picture offensive. Other employees reported receiving from Officer #1 an email with a copy of this same picture. The investigator found evidence in the computer records that proved that Officer #1 had sent such an email to several BPD employees.

Another female employee said that Officer #1 told her, while she was pregnant and working in the same unit as Officer #1, that she should be careful that the weight gain from pregnancy does not cause her to, "lose her ankles."

Some of Officer #1's fellow employees (both female and male) reported that they had mentioned to Officer #1 that they found his comments and emails to be objectionable. Others said that they were not offended and felt that Officer #1 just had a "goofy" sense of humor. One female employee said that, when she first came to work for BPD in the same

unit as Officer #1, she was told by another female employee that Officer #1 says and does things that might be offensive to some, but that she (the new employee) should not worry about it because Officer #1 was a nice guy and did not mean any harm.

As indicated above, an audit of email messages sent by Officer #1 revealed several messages containing offensive or inappropriate content. In addition to the undressed female motorcycle rider, the investigator found an email from Officer #1 to a female BPD employee that contained a picture of an elderly, overweight female in tight shorts with the following message from Officer #1 to the female employee: "Your day is coming!"

Officer #1 confirmed that he sent the emails but could not recall making the comment, "Pull up your pants," from outside the meeting room. He did admit that he regularly complimented female employees on their appearance and sometimes joked around with them. He also said that his fellow employees (both male and female) joked back and made fun of his age and appearance. Officer #1 expressed a belief that all of this was good-natured and that he had no intention of offending anyone or making them uncomfortable.

OMBUDSMAN'S ANALYSIS AND FINDINGS

Alleged Stalking And Telephone Harassment

With regard to Officer #1's behavior, as it relates to the potential criminal violations of stalking (Idaho Code §18-7905) and telephone harassment (Idaho Code §18-6710), the Canyon County Chief Criminal Prosecutor determined that no criminal violation had occurred.

BPD Policy §21.0302 Conformance to Laws states:

Employees shall obey all laws of the United States and of any state and local jurisdiction in which they are present. A conviction for the violation of any law shall be prima facie evidence of a violation of this section. A sustained violation of this section may result in discipline, up to and including termination.

Based on the review completed by the criminal prosecutor for Canyon County, Officer #1 did not violate BPD's Conformance to Laws policy. His relationship and contact with the Complainant, while each described it as difficult, did not include stalking or harassing behavior that would be in violation of the law. Therefore, a finding of unfounded was issued.

Use Of BPD Cell Phone For Other Than Official Business And Failure to Reimburse BPD

Officer #1, for a period of approximately two years, regularly phoned and received calls from the Complainant using his department-issued cellular telephone. The research conducted in this investigation shows that Officer #1, beginning with the billing cycle of May 26, 2002 through the end of billing cycle June 16, 2004, spent at least 35.5 hours on his cellular phone with the Complainant.

BPD Policy §24.1300 Cellular Telephone Calls and Reimbursement states (in part):

Cellular telephones are a valuable business-use tool for BPD to increase efficiency. Employees with assigned cellular telephones shall have their cell phones on and operating during normal duty hours, unless tactical operations dictate otherwise, and shall check the voice message system regularly during duty shift for messages and calls received. Cell-phone numbers will be provided to citizens when appropriate.

Employees will be assigned a block of cellular minutes appropriate for duty use. Employees shall use discretion and consider their billing plans when determining if cellular telephones are the most efficient means of completing activities. When possible, other means of communications (radios, standard telephones, etc.) should be chosen for their cost efficiency. Long-distance calls should always be made from standard telephones, unless extenuating

circumstances exist. Long-distance calls made from cellular telephones will incur extra costs in many cases. Employees should also remember that cellular telephones can be monitored, so the discussion of sensitive issues on the phones should be avoided.

In using his BPD cell phone to call the Complainant, Officer #1 used assigned minutes for purposes that were not duty-related and were outside the scope of duty use. Officer #1 admitted that using his cellular telephone to facilitate his affair with the Complainant was not an acceptable use of department equipment.

During this investigation it was determined that Officer #1 did not fully reimburse the department the actual amount of money owed when he exceeded the calling plan minutes using his BPD cellular telephone. Officer #1's cell phone records and reimbursement history were reviewed from December 26, 2001 through July of 2004. The Cellular Telephone and Reimbursement policy (§24.1300) for 1999 through 2003 was reviewed against Officer #1's reimbursement history. This policy states, in part:

July 1999 - Personal calls on Department-issued cellular telephones are discouraged. Employees shall reimburse the Department for all personal calls that are made.

March 2001 (Special Order) - Cellular phone bills will be reviewed regularly for usage. Employees will be responsible for reimbursing the Department for excess usage that cannot be justified for business purposes.

August 2002 - Cellular phone bills will be reviewed regularly for usage. Employees will be responsible for reimbursing the Department for excess usage that cannot be justified for business purposes.

November 2003 - Cellular phone bills will be reviewed regularly for usage. Employees will be responsible for reimbursing the Department for excess usage that cannot be justified for business purposes.

Officer #1 owed the department approximately \$331. Officer #1 admitted that he did not reimburse BPD for personal phone calls made to the Complainant, but did pay for other personal calls he had made. The Department's policies clearly state consistently that officers

are required to reimburse the department for personal calls that cannot be justified for business purposes. A finding of sustained was issued in connection with this allegation.

Engaging In Non-police Business While On Duty And On-Duty Behavior Likely To Bring Discredit On The Department

Officer #1's sexual contacts with Complainant #2 during on-duty time and his use of a BPD police vehicle were analyzed against the following two department policies :

BPD Policy §21.0120 On-Duty Time Restricted to Police Work states:

Unless otherwise detailed, an officer shall restrict his/her police duties during working hours to his/her assigned duty area. An officer shall not conduct personal business on duty time for the purpose of private gain. Officers shall not engage in personal recreation or entertainment during their tours of duty.

BPD Policy §21.0201 Law Enforcement Code of Ethics and Code of Conduct states (in part):

Officers will conduct themselves, both on- and off-duty, in accordance with the Law Enforcement Code of Ethics and Code of Conduct.

Code of Ethics (second paragraph):

I will keep my private life unsullied as an example to all and will behave in a manner that does not bring discredit to me or to my agency. I will maintain courageous calm in the face of danger, scorn, or ridicule; develop self-restraint; and be constantly mindful of the welfare of others. Honest in thought and deed both in my personal and official life, I will be exemplary in obeying the law and the regulations of my department. Whatever I see or hear of a confidential nature or that is confided to me in my official capacity will be kept ever secret unless revelation is necessary in the performance of my duty.

Code of Conduct (Private Life):

Police officers will behave in a manner that does not bring discredit to their agencies or themselves. A police officer's character and conduct while off

duty must always be exemplary, thus maintaining a position of respect in the community in which he or she lives and serves. The officer's personal behavior must be beyond reproach.

Officer #1 admitted that in November 2002, while he was on-duty, he took a trip above the Lucky Peak Dam in his police car with Complainant #2, for the purpose of looking at her undergarments. During that trip, neither dispatch nor other BPD employees could contact Officer #1 because cell phone, two-way radio, and pager services are not available in the area visited by Officer #1 and Complainant #2. Officer #1 was clearly engaged in personal recreation or entertainment during that trip past Lucky Peak.

Officer #1 admitted that he and Complainant #2 had sexual contact in his home during the work day on several occasions. While it could be argued that this was purely private behavior engaged in during Officer #1's lunch break from work, it was facilitated by his use of a BPD cell phone to arrange the meetings and a BPD police vehicle to travel to and from them. In addition, Officer #1 represented himself to an entire patrol shift as being on-duty during the evening of July 26, 2003, when, in fact, he and Complainant #2 were engaged in sexual activity for two or three hours in a Boise hotel. While Officer #1 had some flexibility regarding the hours he worked and was not required to work that particular patrol shift, he chose to attend the shift briefing in uniform and make it clear to the other officers that he would be out on patrol during the shift. This clearly indicated to the other officers on-duty at that time that Officer #1 was also on-duty and available for police duties. However, about an hour after the shift began, Officer #1 met Complainant #2 and they spent the next two to three hours in a hotel room engaged in sexual activity. Following this, Officer #1 returned to his police vehicle and went on patrol for the remainder of the shift.

Having voluntarily presented himself to fellow officers and supervisors as being on-duty, Officer #1 had an obligation to remain on-duty until such time as he notified them that he was no longer in service. Instead, Officer #1 abandoned his self-imposed duty for the sake of a sexual encounter, while failing to inform his fellow officers that he was no longer available

to assist them. Therefore, two sustained findings were issued for violation of §21.0120 and §21.0200.

Release Of A Confidential Password To The Complainant

Policy requirements for confidentiality are addressed in BPD Policy §21.0317:

No employee shall divulge, without proper authority, any confidential information obtained in the course of employment with the department. Confidentiality applies to information or events that an employee reads, sees, or hears. Confidentiality also applies to information to which an employee can grant access.

Complainant #2 alleged that Officer #1 provided her with his MDT password. Officer #1 denied ever sharing his MDT password with Complainant #2. The investigation failed to discover sufficient evidence to clearly prove or disprove the allegation made by the Complainant. A finding of not sustained was issued. A “not sustained” finding means that the preponderance of the evidence neither proved nor disproved that a violation of the policy occurred.

Use Of Official Position To Receive Discounts

The allegation that Officer #1 received discounts from area hotels based on his position within BPD was reviewed against BPD’s policies regarding discounts and the ethics of an officer’s official position.

BPD Policy §21.0209 Bribes, Discounts, Gratuities, Rewards, And Gifts states (in part):

All employees shall conduct themselves in a manner that will not bring discredit upon themselves or the Boise Police Department. This prohibits the solicitation and/or acceptance of any bribe and any discount, gratuity, reward, or gift that could, in the public mind, be interpreted as capable of

influencing an employee's judgment in the discharge of duties or that would reflect favoritism by the employee or Department toward any particular person, group, or business.

BPD Policy §21.0202 Ethics of Official Position states (in part):

It shall be the policy of the Department that its officers use their positions as sworn law-enforcement officers only for the purpose of accomplishing their assigned duties, with the goal of serving and protecting the citizens of Boise and their property. Officers of this Department shall not use their position as a means of personal gain, personal favor, or personal influence. Furthermore, officers shall avoid involvement in any endeavor which may reasonably constitute a conflict of interest with their position as an employee of the department.

- a An officer shall not use his/her official position, official identification cards, or badges:
 - 1 For personal or financial gain.*
 - 2 For obtaining privileges not otherwise available to them, except in the performance of duty.**

While Officer #1 did receive discounts at two area hotels, the preponderance of evidence does not indicate that he was provided those discounts based on his position with BPD. He was given discounts available to anyone who knows, is associated with, or is related to an employee of either hotel, based on the personal relationships he had developed with hotel employees. Each hotel has standards by which they determine the rate of discount to be given. When a discount request is made, the hotels determine whether or not the discount will be provided based on factors such as room availability and time of year. Based on the evidence, a finding of unfounded was issued.

Unauthorized Use Of BPD Computer Equipment And Internet Access

The investigation produced a preponderance of evidence proving that Officer #1 used a computer owned by the City and assigned to him by BPD for purposes not related to BPD business and expressly prohibited by policy.

BPD Policy §21.0501 Personal Use of Any Computer Equipment or Software states (in part):

Personal use of any Department-owned computer equipment or software is not authorized. Personal use constitutes anything that is not job-related. The Department reserves the right to monitor or access all electronic messages and files.

BPD Policy §21.0502 Use of Internet and E-mail states (in part):

Access to the Internet or E-mail services via Department-owned equipment or communication links is for official business only. Examples of appropriate use include research for specific job-related objectives, communication with peers on officially recognized issues, and exchange and sharing of job-related information. Inappropriate use encompasses anything that is not directly job-related. Unless approved by the appropriate supervisor as a specific part of an investigative activity, the following uses of the Internet, using Department equipment or facilities, are not allowed:

- *Access, retrieval, or printing of text and/or graphics information which exceeds the bound of generally accepted standards of good taste and ethics. Pornographic sites shall not be accessed.*

Officer #1's personal use of his computer included regularly receiving and sending email messages that were not job-related. Many of these messages contained sexual or otherwise offensive content. In addition, Officer #1 used the internet access provided to him by BPD for viewing pornographic material. This behavior was not authorized by BPD and was unconnected to Officer #1's official duties. Officer #1 also used his BPD-provided internet access to download and store on the BPD computer assigned to him a graphically pornographic video. Finally, Officer #1 made regular and extensive use of BPD internet

access to visit sports and entertainment sites having no connection to his assigned police duties. As a result, two sustained findings were issued for violating these policies.

Use Of Other BPD Employees To Perform Work Related To Outside Employment
Unauthorized Use Of BPD Computer Equipment And Internet Access

City of Boise policy articulates to employees the ethical conduct and fiduciary duty they owe the citizens. The Code of Ethics and Fiduciary Duty (Boise City Policy §7.28) states (in part):

Fiduciary Duty:

Every City employee owes a fiduciary duty to the City of Boise and to the Citizens of the City of Boise. This fiduciary duty is defined as a duty to act for the benefit of the citizens of the City of Boise, while subordinating one's personal interests to those of the City as a whole. When an employee expends any resources of the City, this fiduciary duty requires that the expenditure be reasonable, prudent and for the benefit of the City and not for personal gain. It is the highest standard of duty implied by law and is required by this policy.

Standard of Conduct:

No City employee shall knowingly:

Use his official position or office to obtain financial gain for himself, any member of his household, or any business with which he or a member of his household is associated.

Officer #1 held a position of employment with an outside employer, other than the City of Boise. On two occasions, Officer #1 directed two BPD employees under his supervision to work on projects related only to his outside employment. These tasks had no connection to the business of the Boise Police Department, or the duties assigned by BPD to those two employees. The two employees worked on Officer #1's outside tasks during their regular BPD work hours. This took time and resources away from BPD work activities for approximately six hours. This use of BPD human resources was not for the benefit of the

City as whole and was specifically for Officer #1's personal gain. As a result, a sustained finding was issued.

Making False Statements In An Ombudsman Investigation

The department maintains a strict policy regarding the truthfulness standard for its employees. BPD and the City of Boise have established a policy that directs employees to be truthful. That policy specifically states that employees are required to be truthful during an investigation conducted by the Office of Internal Affairs (OIA), a supervisor, or the ombudsman's office. The department's policy (§22.0110) states (in part):

Employees shall truthfully and completely answer all questions specifically directed and related to the scope of employment and operations of the Department that may be asked of them by any OIA investigator, supervisor, or by the Ombudsman's Office.

Untruthfulness in any of the following situations shall be considered grounds for termination:

- *Untruthfulness regarding material facts during any internal investigation, including investigations conducted by or on behalf of the Ombudsman's Office.*

Officer #1 was directly asked, during his second interview with the assistant ombudsman, whether or not he had accessed pornographic material using his assigned BPD computer. He denied this and said that someone else had downloaded the material to his computer and then he accessed "three pop-ups." Officer #1 was also asked if he downloaded a pornographic video. He said he had seen, but not downloaded, a video of an old woman and described the old woman as being about 75 years old. Officer #1 also claimed that several other BPD employees had the password to his user name on the computer system.

In his third interview with the assistant ombudsman, Officer #1 admitted that he had viewed pornographic web sites and downloaded a pornographic video. He admitted that he had not

been truthful with the assistant ombudsman during her second interview of him. As a result, a sustained finding was issued.

Failure To Follow Required Computer Security Practices

BPD's Computer Security Practices policy (§21.0504) states (in part):

Employees shall take whatever steps he/she can to protect our systems and the valuable information they contain. The following is a list of steps that each user should take to help keep our systems safe from unauthorized access:

Always log off. All employees are required to log off at the end of their shift. If possible, you should also turn off your system. Your screen saver should be password protected if you plan on leaving your computer unattended for a period of time during the work day.

Officer #1 admitted that he had not routinely or consistently logged off his computer. He also had not secured his office by locking and shutting the door. At least three of Officer #1's fellow employees secured his office for him on a number of occasions. It was common knowledge within the department that Officer #1 did not take reasonable steps to ensure that his office and computer access were secure. In fact, Officer #1 stated that he wanted to create an atmosphere of openness and accessibility. While such a philosophy is commendable, creating an atmosphere of openness and accessibility could have been accomplished without leaving his computer and office unsecured. A sustained finding was issued.

Unauthorized Release Of Confidential Police and Personnel Information

Officer #1 sent a number of email messages that included confidential police and personnel information. According to the department's Confidentiality policy (§21.0317):

No employee shall divulge, without proper authority, any confidential information obtained in the course of employment with the department. Confidentiality applies to information or events that an employee reads, sees, or hears. Confidentiality also applies to information to which an employee can grant access.

Officer #1 admitted that he sent, via email, confidential police and personnel information to a person who was not employed by BPD. Officer #1 admitted that he did so without the authority to do so and that he had obtained the information in the course of his employment with BPD. A finding of sustained was issued.

Workplace Harassment

BPD Policy §21.0308 deals with harassment in the workplace. This policy states:

All employees, regardless of their status of employment, have a right to work in an environment free from intimidation, ridicule, or harassment based on gender, race, color, age, religion, sexual orientation, or national origin. Workplace or other harassment, including retaliation against employees who report harassment, constitutes illegal employment discrimination, is unacceptable conduct in the workplace, and will not be tolerated. Where it is found to exist, immediate corrective action will be taken to assure it is stopped and does not recur. Employees who commit workplace or other harassment or retaliatory acts shall be subject to disciplinary action, up to and including dismissal. (See Boise City Employee Policy Handbook, 1.04 Harassment.)

Boise City Policy §1.04 Harassment states (in part):

Definition of Prohibited Behavior:

b) Hostile Work Environment is at issue:

*Such conduct has the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating, hostile or offensive working environment through discrimination, intimidation, ridicule or insult (Please note: "Hostile Work Environment" applies to **all** types of harassment).*

*“Unwelcome” is determined by the recipient of the behavior, **not** the alleged perpetrator.*

Examples of Other Harassment:

II) Other Harassment:

(2nd Paragraph) General Workplace Harassment is a form of offensive treatment or behavior, which to a reasonable person creates an intimidating, hostile, or abusive work environment. Examples can include but are not limited to: Verbal or physical behavior which is derogatory, abusive, bullying, threatening, or disrespectful behavior, ridiculing or undermining an individual with vindictive or humiliating words or acts.

*The list below includes some examples of social behaviors that foster a **hostile work environment** and are inappropriate and unacceptable on the job:*

Communicating stories, jokes, etc. containing sexual, racial or ageist material. Use of slurs or slang names meant to put down persons of a particular race, age, sex, ethnic or religious background. This includes communicating such material verbally, in writing, by e-mail, or voice mail.

Displaying and/or distributing printed material of any nature which stereotypes or demeans persons of a particular race, age, sex, ethnic or religious background. Suggestive looks or leering, “undressing with eyes.”

Officer #1 routinely complimented female employees regarding their outfits, shoes, hairstyles, and perfume. While female employees stated they were not offended by his compliments and many found his compliments to be thoughtful, there was a general awareness that Officer #1's compliments were not always appropriate for the workplace. One female employee even warned a newly-hired female employee that Officer #1 might say things that could be considered unusual in the workplace.

One female employee reported that she was offended by a comment made by Officer #1. The comment was inappropriate and outside the generally accepted standards of a professional workplace. Officer #1 also sent two photographs, via email, to the same female employee. These photographs depicted the bare buttocks of two females. In one of these

email messages, Officer #1 wrote that the employee's day was coming when she would look like the female in one of the photos. Based on the picture, it was reasonable to conclude that this comment was not complimentary. A second employee was also offended when he received an email with a picture of a woman's bare buttocks.

Other employees were also aware of Officer #1's "communication style" and reported having informal discussions with him about it. It is clear that Officer #1 developed a pattern of behavior that was tolerated and excused by the employees around him, including management personnel. Even though Officer #1's behavior had been tolerated by fellow employees and supervisors, this pattern of behavior clearly created a potentially hostile work environment. Therefore a sustained finding was issued.

OMBUDSMAN'S POLICY RECOMMENDATIONS

In light of what was found during this investigation, the ombudsman made the following policy and training recommendations to the chief of the Boise Police Department:

Harassment Policy Training

Given what was learned in the course of this investigation, particularly regarding inappropriate and questionable behavior that had been widely known but not directly confronted, BPD supervisors may benefit from additional training regarding their obligations to implement and enforce Boise City's harassment policy. The harassment policy dictates strict requirements for supervisory response to such behavior in order to protect employees from behavior that is, or could become, harassment. This policy is also designed to protect the city and its departments from the liabilities associated with violations of the harassment policy. It is recommended that the department review and improve (if necessary) its training and communication of this important policy area.

Cell Phone Reimbursement

It is recommended that BPD's practice regarding cell phone reimbursement be evaluated. It appears that the current policy requirement regarding reimbursement is not being consistently and strictly enforced. This use of public funds for personal purposes, in the form of un-reimbursed charges for cell phone time over the pre-paid plan, must be discouraged.

Administrative Leave Letters

It is recommended that BPD require its supervisors to use a standard letter when placing employees on administrative leave. When an administrative investigation is underway and it becomes necessary to place an employee on administrative leave, correspondence to the employee should clearly state that he or she is being placed on administrative leave with pay and that this action is non-punitive and non-evaluative. Such correspondence should also clearly state that the affected employee is to have no contact (whether in person, via telephone, by email, or in any other form) with department employees other than a designated contact (generally the direct supervisor). It is also recommended that access by the employee on leave to email, any Boise City computer system, and all City facilities without public access be blocked while he or she is on administrative leave.

Email Audit

It is recommended that BPD conduct an immediate audit of email activity by and among its employees. Certain content, such as that found in the course of this investigation, can be a violation of email and harassment policies. Our review of only one email account (that of Officer #1) indicates that the sending and receipt of inappropriate emails was not limited to that one individual.

Internet Access

This investigation revealed that a significant number of computer users at BPD have unrestricted and unmonitored access to the internet. It is recommended that BPD review the advisability and necessity of unrestricted internet access by any BPD employee. While legitimate investigative and department business may necessitate the granting of such access, this should be done on an extremely limited basis. Furthermore, it is recommended that BPD institute a policy and practice of regularly auditing any computer accounts granted unlimited internet access. Doing this will help ensure that the viewing of pornographic or otherwise objectionable material is strictly limited to instances where legitimate police business requires it.

Pierce Murphy
Community Ombudsman
P.O. Box 500
Boise, Idaho 83701-0500
(208) 395-7859
mailbox@boiseombudsman.org