



STATE OF WASHINGTON  
DEPARTMENT OF SOCIAL AND HEALTH SERVICES

PO BOX 88450  
Steilacoom, WA 98388-0646

September 20, 2012

CONFIDENTIAL

CERTIFIED/REGULAR MAIL

Sammie Neely

RCW 42.56.250(3)

Washington 985

**SUBJECT: Notice of Dismissal**

Dear Mr. Neely:

In accordance with the provisions of the Master Agreement (MA) between the State of Washington and the Washington Federation of State Employees, this is official notification of your dismissal from your position as a Residential Rehabilitation Counselor 2 (RRC 2) with the Department of Social and Health Services (DSHS) at the Special Commitment Center (SCC) **effective September 22, 2012**. This action is a result of your personal use of the state's computer system; specifically your use of your assigned computer and the internet for your own personal use including accessing pornographic web sites.

**Basis for Potential Discipline**

On March 8, 2012, the SCC IT department provided Mark Davis, Administrative Services Chief, a Computer Exam Report of the computer assigned to you, in the Cedar Unit. The report listed 103 unauthorized and non-work related sites visited by you during February and March 2012.

On March 13, 2012, Mr. Davis assigned Darold Weeks, Chief Investigator, to investigate the 103 unauthorized visits. Mr. Weeks was given a copy of the Computer Exam Report of the 103 unauthorized visits made by you using your assigned computer, number A530467. On April 12, 2012, Mr. Weeks scheduled a meeting with you regarding the alleged misuse of the state's computer systems.

**Investigative Meeting**

On April 20, 2012, Mr. Weeks met with you. The interview was originally scheduled for 8:00 a.m. and was rescheduled at your request to the earlier time of 7:00 a.m. Prior to the interview, you asked Mr. Weeks if you needed Union Representation, and you were informed that it was your choice. You were asked if you wanted to reschedule to seek representation, and you indicated that you did not need representation.

During the interview you admitted to using your assigned state computer for the following:

- To create a password for your Skype account for your cellular telephone so you could contact your son in Afghanistan.

Sammie D Neely 9-21-12



- You checked your bank account a couple times.
- You checked military sites trying to locate your son.

During the meeting, Mr. Weeks provided you time to review the Computer Exam Report of the Cedar Unit computer assigned to you, number A530467. This report listed 103 entries attributed to your User Profile (Neelysj) for your assigned computer use during February and March 2012.

Of those entries, there were 35 or more identified as associated with "Livejasmin". You were asked to review the documentation and mark the entries that were job related. At the conclusion of your review, you said, *"This Livejasmin, I don't know what this is. Honest to god I have no clue what that is. Nothing I'm seeing here is job related. I have no idea what Livejasmin is."*

You were provided with a copy of the screen shot of the site listed as "Livejasmin". The site is advertised as "The World's #1 Most Visited Video Chat Community—Free Live Sex Video Chat."

After reviewing the document you commented "that must be a pop-up. I've only gone to those sites I told you about. I've never left the computer when I was logged on and I've never gone to an adult site." You were asked if you had an account with Livejasmin and you responded "No I don't. I've never visited that site."

On May 3, 2012, Heather Sacha, ITAS6, was asked if the site listed as "Livejasmin" in the Neely report could have been "pop-ups."

Ms. Sacha conducted a Google search of the site Livejasmin.com on March 8, 2012, and learned the site is a Live Sex and Chat Room website. Ms. Sacha reported that since the site is live it is impossible to recreate what was viewed by you. She also reported that no video pop-ups were encountered during her visit to the site.

Ms. Sacha conducted a Field Search examination of your Internet use and during a review of the Internet history data learned the following:

- You conducted several page visits within the site Livejasmin.com.
- Several swf files (video files) loaded during your visit to the Livejasmin.com site on February 14, 2012.
- The initial Livejasmin.com page loaded and then 4 minutes later another page with different graphics loaded along with free.chat.css.
- Members.Livejasmin.com, a webpage for paying members only, was also visited by you, using your assigned state computer, on October 10, 2008.

On May 10, 2012, Mr. Weeks received a Summary Report from Heather Sacha clarifying your computer usage which included the above information:

As part of the fact finding, Mark Davis, Administrative Services Chief, instructed Jill Swick, Administrative Assistant 3 (AA3), to research the website "Livejasmin.com". Ms. Swick accessed the sites homepage, clicked on the category titled "couples" and a screen with

approximately 15-20 live video streams of various nude couples and women engaging in sexual activity appeared.

Next to each video was a "Free Chat" button. Ms. Swick reported she clicked on the button for the 1<sup>st</sup> video and immediately a live broadcast loaded revealing a couple performing sexual acts on one another. After approximately 45 seconds, Ms. Swick exited the site and was routed back to the screen with the 15-20 live pornographic videos.

Ms. Sacha reported that the "test site visit" conducted by Jill Swick revealed findings similar to the findings on your computer as listed in the Computer Exam Report. It displayed:

- The same SWF (video flash files)
- sowriter.swf (#9),
- memberchat346.swf (#10)
- freechat.css (#18)

On April 24, 2012, you gave a hand written note to Mr. Weeks. In the note, you wrote, "I am writing this statement in regards to the meeting that took place on 4-20-12. At that time all of my internet usage was gone over. I stated then and I am stating now, that I did not knowingly or willingly visit or log into any web sites that are Adult or Immoral in nature."

#### **Policies and Procedures Implicated**

As a DSHS employee, you are required to complete the Employee Annual Review Checklist process, which includes your review and adherence to all agency policies included on the checklist. On January 13, 2011 and October 29, 2011, you acknowledged you had read, understood and would comply with Administrative Policy (AP) 18.64 "Standards of Ethical Conduct for Employees" and AP 15.15 "Electronic Messaging System and the Internet."

DSHS Administrative Policy 18.64, "Standards of Ethical Conduct for Employees" states in relevant part:

#### **A. Required Standards of Behavior and Conduct**

All DSHS employees, contractors, and volunteers are required to perform their duties and responsibilities in a manner that maintains standards of behavior promoting public trust, faith, and confidence as described below:

2. Promote an environment of public trust free from fraud, abuse of authority, and misuse of public property.
3. Strengthen public confidence in the integrity of state government by demonstrating the highest standards of personal integrity, fairness, honesty, and compliance with law, rules, regulations, and DSHS policies.
6. Comply with the requirements of this policy. Failure to comply with requirements of this policy may result in disciplinary action up to and including discharge from employment.

DSHS Administrative Policy 15.15 "Electronic Messaging System and the Internet" states in relevant part:

### C. Employee Use of Electronic Messaging Systems and the Internet

1. **Permitted Business Use** - Employees may use department provided electronic messaging systems and Internet access to conduct business that is reasonably related to official state duties, to include electronic recruiting and Employee Self Service.

Employees represent DSHS when using electronic messaging systems and accessing the Internet to conduct state business. Employees must use these tools in accordance with Administrative Policy 18.64, Standards of Ethical Conduct for Employees.

2. **Permitted Personal Use** – Personal use of department electronic messaging systems and the Internet must conform to WAC 292-110-010, Use of State Resources, which states that employees may make occasional and limited personal use of state resources, such as electronic messaging systems and the Internet, if the use conforms to all of the following ethical standards:

- a. There is little or no cost to the state;
- b. The use does not interfere with the performance of the employee's official duties;
- c. The use is brief in duration and frequency. Employees are expected to exercise good judgment in both duration and frequency;
- d. The use does not disrupt other state employees and does not obligate them to make personal use of state resources; and
- e. The use does not compromise the security or integrity of state information or software.

Prior to engaging in limited personal use of state resources, employees are encouraged to seek guidance from their supervisor as to whether the intended usage is considered to be de minimis.

3. **Prohibited Uses** – Employees are prohibited from using state-provided electronic messaging systems and the Internet in any of the following ways:
  - a. Personal use of state-provided electronic messaging systems or Internet access that does not meet the conditions found in C.2.a-e above is prohibited.
  - d. Employees must not use state-provided electronic messaging systems, faxing, scanning, or Internet access to create, access, post, send, or print any pornographic material unless the material is necessary for the performance of the employee's job-related duties (e.g., when necessary for conducting an investigation). If such use is necessary for the performance of job-related duties, employees must get written permission from their supervisor authorizing such use.
  - e. Department employees must not use state-provided Internet sites, faxing, scanning, or copying to create, transmit, or store electronic messages that

contain or promote:

- 7) Any activity that is prohibited by federal, state, or local law, or department policy.
- f. In addition, employees may not use state-provided Internet access, to:
- 3) Participate in non-work related Instant Messaging, chat groups, listservs, blogs, or newsgroups;
  - 7) Link DSHS web sites to other Internet sites in violation of Administrative Policy 15.18;
- h. Employees must not establish an Internet connection (e.g., AOL, MSN, etc.) to or from a computer connected to the department network that bypasses the Washington State Department of Information System (DIS) firewall.
- j. Using instant messaging provided by an external vendor is prohibited. This includes instant messaging solutions offered by vendors such as Microsoft, AOL, and Yahoo.

While using the Internet, if at any time an employee inadvertently accesses an inappropriate site, the employee should immediately close the page and notify his or her supervisor.

#### **A. Disciplinary Action for Noncompliance**

- A.** Violations of this policy may result in disciplinary action, up to and including termination from state employment. In addition, there may also be separate actions against an employee for violation of the state's ethics laws such as letters of reprimand, fines, civil actions, and criminal prosecution.
- B. Pornographic Materials:** DSHS has a zero tolerance regarding pornographic material in the workplace. If, after an investigation, it is found that an employee used state resources to create, access, post, transmit, print, or store pornographic materials not appropriate for the workplace, the most stringent disciplinary action will be taken.
- C. Sexually Explicit Materials:** If, after an investigation, it is found that an employee used state resources to create, access, post, transmit, print, or store sexually explicit materials not appropriate for the workplace, appropriate disciplinary action will taken, up to and including termination from DSHS employment. The administrations highest-level appointing authority will consult with the Senior Director of DSHS Human Resources to determine the level of disciplinary action taken.

An All Staff Memo sent by Cathi Harris, Associate Superintendent, dated October 2, 2008, which states in relevant part:

The IT department has diagnosed and reported to me several network bandwidth problems that are resulting in lack of resources. You are directed to stop these types of

computer uses as well as any other uses that violate SCC Policy 926 and DSHS Policy 15.15. Further violation of these policies may result in disciplinary action.

Additionally, on February 8, 2010, Kelly Cunningham sent a memo to all staff titled "Computer and Electronics Usage Directive" to remind all staff assigned to the SCC to comply with agency policies regarding appropriate computer usage and, which included the following bullets:

- Please remember to follow guidelines and policies on internet use. Please note there is ZERO TOLERANCE of any employee accessing pornographic material.
- In addition . . . Employees who violate these policies may be subject to disciplinary action, up to and including dismissal from employment as well as separate actions from state ethics law violations, possible criminal or civil prosecution.

#### **Pre-disciplinary Meeting**

A pre-disciplinary meeting was scheduled with you on Thursday, August 16, 2012 at 2:30 p.m. in the administrative office in Steilacoom. In attendance at the meeting were you, Steve Chenoweth, Council Representative; Mark Davis, Administrative Services Chief; and Walter Bracy, Human Resource Manager. During this meeting you admitted that you had used the computer for personal reasons to use Skype to attempt to contact your child overseas. You then stated you were on resident EF watch around 6:00 a.m. on the date in question, February 14, 2012. Mr. Chenoweth then stated that the times listed on the computer report did not correspond to times that you were on shift. Mr. Davis committed to doing some additional research and sharing that information with Mr. Chenoweth after the meeting. You clearly stated you had never accessed pornographic materials at work. Mr. Davis responded to the follow-up items via email to Mr. Chenoweth on August 27, 2012. The two items for follow-up were whether Mr. Neely was at work at the times in question on February 14, 2012 and what time Mr. Neely was on EF watch on February 14, 2012.

Mr. Davis confirmed the access to the pornographic site "Live Jasmine Live Sex" occurred between 1:25 a.m. and 1:50 a.m. local time on February 14, 2012. These times were determined based on Access times on the report. The access times reflect when the website was last visited by the logged in user. The date and time is provided by the web server that is hosting that website, and it is given in Universal Coordinated Time, also referred to as "UTC Time." SCC reports use website server URL - UTC time to prevent data manipulation because a local user cannot manipulate the Server URL information which includes the UTC time and date of visit. UTC time is based on the Prime Meridian (Greenwich England) date/time when the web site was accessed. This event occurred on February 14, 2012, so standard time applies to the conversion of UTC time to Local Time because in this year daylight savings time did not begin until March 11<sup>th</sup>. To convert UTC time to Pacific Standard Time for February 14, 2012, we must subtract 8 hours from the stated UTC time/Date on the IT computer report. In subtracting the 8 hours from the UTC time, it appears that most of the alleged computer misuse, including Mr. Neely's admitted visits to Skype and his visits to Live Jasmine Live Sex web site, occurred sometime between 1:25 a.m. and 1:50 a.m. on the morning of February 14, 2012.

Mr. Davis also reviewed the EF watch record for February 14, 2012 and Mr. Neely was not on EF watch from 1:25am to 1:50am.

Mr. Davis also reviewed Mr. Neely's attendance record on February 14, 2012 and verified Mr. Neely was at work from the hours of 12am to 8am.

**Determination**

In determining the appropriate level of discipline, I have carefully reviewed and considered all the facts regarding the incidents listed above and have reviewed your personnel file and your 5 year employment history. DSHS Administrative Policy 15.15 is very clear regarding disciplinary action for noncompliance, "Pornographic Materials: DSHS has a zero tolerance regarding pornographic material in the workplace. If, after an investigation, it is found that an employee used state resources to create, access, post, transmit, print, or store pornographic materials not appropriate for the workplace, the most stringent disciplinary action will be taken."

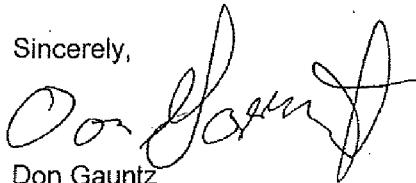
The investigation substantiated that you were on duty at the times reflected in the computer report. You were not at any other location. I do not find your responses credible and your behavior as outlined above is unacceptable. I believe that retention of your employment with the SCC would be a demonstration of poor judgment on my part in the stewardship of the public's trust placed in me as the appointing authority over an institution that cares for and ensures security of civilly-committed adult, violent sexual predators. I have determined I have no other recourse than to dismiss you from employment.

Please make arrangements with your supervisor to return all State issued equipment that may be in your possession, including your identification badge and uniforms.

I have attached an EAP pamphlet as a resource for you. Their services are free to state employees and they may be reached in Olympia at 360-753-3260. For additional information you may go to their website at [www.dop.wa.gov/EAP](http://www.dop.wa.gov/EAP).

Pursuant to Article 29 of the above referenced Collective Bargaining Agreement, you may grieve this action.

Sincerely,



Don Gauntz  
Interim CEO  
Special Commitment Center

cc: Cathi Harris, Residential and Security Operations Chief  
Melissa Lovell, PA1 Manager  
Margaret Maddox, Chief, HR Operations  
Sue Thomas, Human Resource Administrator  
Steve Chenoweth, WFSE Council Representative  
Personnel File

---

Sammi Neely  
Acknowledgement of Receipt

---

Date