BEFORE THE GOVERNING BOARD OF THE

FALLBROOK UNION ELEMENTARY SCHOOL DISTRICT

FALLBROOK, CALIFORNIA

In the Matter of the Dismissal of ELAINE ALLYN, a Senior Management Classified Employee	**NOTICE OF CHARGES THAT THERE EXISTS CAUSE TO DISCIPLINE A SENIOR MANAGEMENT CLASSIFIED EMPLOYEE, ELAINE ALLYN**

TO THE GOVERNING BOARD OF THE FALLBROOK UNION ELEMENTARY SCHOOL DISTRICT:

I, Dennis Bixler, Assistant Superintendent, Human Resources, of the Fallbrook Union Elementary School District ("District"), Fallbrook, State of California, pursuant to Education Code section 45113 and Board Policy 4218, hereby file with the Governing Board of the District the following Statement of Charges in Recommendation of Immediate Suspension Without Pay and Dismissal of Elaine Allyn, a senior management classified employee of the District.

CHARGES

There exists cause for the immediate discipline of Ms. Allyn in that she has demonstrated dishonesty, engaged in immoral conduct, misuse of district property, violations of district policies and procedures and failure to comply with school laws of the state and federal governments. (District Board Policy 4218 sections (f), (k), (o), and (p).) In particular, Ms. Allyn has violated District Board Policies 4040, 4219.21, 4300, 4319.21, District Administrative

Regulation 4040, school laws of the state and federal governments, including, but not limited to, 18 U.S.C. § 1001, 47 U.S.C. §§ 254, 502, 503 and 47 C.F.R. §§ 516, 54.500, et seq. Ms. Allyn's dishonesty, immoral conduct, misuse of district property, violations of district policies and procedures, and failure to comply with school laws of the state and federal governments is evidenced by Ms. Allyn hacking into administrator e-mail accounts, perpetrating fraud upon the District, destroying evidence of her wrongful activities, and mishandling the District's E-rate program.

STATEMENT OF FACTS

Dishonesty; Immoral Conduct; Misuse of District Property; Violations of District Policies and Procedures and Failure to Comply with School Laws of the State and Federal Governments.

(District Board Policy 4218 Sections (F), (K), (O), and (P).)

1. The District's computer/internet network is run using the product, Netware, which requires each District employee to enter a personalized login name and password to access the District's network. Upon entering the network, an employee may access the internet only by again entering a personalized login name and password. In order to access e-mails, District employees must access the "Groupwise" program, which is installed on District computers and enter another username and password.

2. Ms. Elaine Allyn is responsible, as the District's Director of Information Systems, to collect, store and keep secure the login names and passwords of all District employees. Ms. Allyn is also responsible for ensuring that the District's internal network is maintained and secure. Additionally, she is responsible for complying with the Federal Communications Commission's (FCC) E-rate program requirements.

Unauthorized Access of District Administrator E-Mail Accounts

3. Beginning in the summer and the fall of 2011, shortly after arriving at the District, District Superintendent Candace Singh began noticing that Ms. Allyn was able to anticipate her questions and concerns before Ms. Singh voiced them. Ms. Allyn also reacted to problems before they were brought to her attention. These problems had only been brought to the attention

of Ms. Singh via an e-mail message and could only have been known to Ms. Allyn if she was hacking into the e-mail account of Ms. Singh.

4. On April 20, 2011, a memo was sent to Ms. Allyn which reminded her to complete evaluations for employees under her direct supervision. A copy of the April 20, 2011 memo is attached as Exhibit A.

5. On September 15, 2011, Assistant Superintendent of Human Resources, Dennis Bixler, sent an e-mail to Ms. Allyn reminding her to complete evaluations for employees under her direct supervision. A copy of the September 15, 2011 e-mail is attached as Exhibit B.

6. As of October 28, 2011, Ms. Allyn had still failed to complete evaluations for the employees under her direct supervision.

7. On October 28, 2011, Mr. Bixler sent an e-mail to Superintendent, Ms. Singh; Assistant Superintendent of Educational Services, Eric Forseth and Associate Superintendent, Ray Proctor. The e-mail contained a draft of a Letter of Reprimand directed to Ms. Allyn for her failure to complete evaluations for employees under her direct supervision.

8. On October 31, 2011, Ms. Allyn called at least one of her subordinates into her office for an unscheduled evaluation conference.

9. On or about October 31, 2011, a sealed envelope containing the evaluations for all the employees under Ms. Allyn's direct supervision was received by Mr. Bixler. All the evaluations were signed and dated October 31, 2011. Mr. Bixler informed Ms. Singh, Mr. Forseth and Mr. Proctor about the incident. Later, in February 2012, Ms. Allyn denied reading Mr. Bixler's October 28, 2011 e-mail regarding the proposed Letter of Reprimand. Based upon her conduct, Ms. Allyn's statements are implausible.

10. In or about November 2011, Ms. Singh and Mr. Forseth suspected that someone had been hacking into their accounts and reading their e-mails. They discovered this issue because some e-mails they had not yet read had been marked as "read" in their e-mail inbox. Ms. Singh contacted Ms. Allyn, reported this problem and asked her to remedy it by changing her e-mail password. Ms. Singh requested that Ms. Allyn not save her e-mail login password on paper, which was Ms. Allyn's usual practice.

11. On or about January 16, 2012, Ms. Wendy Hill, a District principal, sent an e-mail to Ms. Singh regarding Ms. Allyn's job performance. This e-mail was not sent to or shared with Ms. Allyn. Yet, just hours later Mr. Forseth and Ms. Singh received unsolicited e-mails from Ms. Allyn, explaining the deficiencies in Ms. Allyn's job performance that had been the subject of Ms. Hill's e-mail. For Ms. Singh, receiving the e-mail from Ms. Allyn before Ms. Singh notified Ms. Allyn of complaints against her, was a significant factor in cementing Ms. Singh's long-standing suspicion that Ms. Allyn had been snooping in Ms. Singh's e-mail box.

12. Based upon the foregoing, an investigation was initiated regarding Ms. Allyn's use of the District's computer system. Specifically, research was conducted regarding the District's computer system and its applications. The investigation also reviewed the contents of a computer used by Ms. Allyn located in the Education Technology (ET) department of the District office.

13. In early February 2012, Ms. Allyn was told to expect a call from an investigator regarding a District teacher and to assist in the investigation in any way she could. On February 7, 2012 a telephone call was placed by the investigator to Ms. Allyn at mid-morning and a message was left, but no return call was received from Ms. Allyn. Following a conversation between the investigator and Ms. Singh about Ms. Allyn failing to return the investigator's call, the investigator sent an e-mail to Ms. Singh that was mildly critical of Ms. Allyn's failure to return the investigator's call. The e-mail was not copied to Ms. Allyn. This e-mail was sent at 6:11 p.m. on February 7, 2012.

14. On February 8, 2012 at 6:47 a.m., Ms. Allyn accessed Ms. Singh's e-mail account through a proxy created for Ms. Singh's assistant, Pat Dales. This unauthorized intrusion took place from Ms. Allyn's residence, which has an IP address of 76.176.206.214.

15. Soon thereafter, on February 8, 2012 at 6:52 a.m., Ms. Allyn sent an e-mail to Ms. Singh informing her that the investigator had contacted her, but she had received the message late in the day.

16. On February 8, 2012 at 7:32 a.m., Ms. Allyn telephoned the investigator and left a message that was apologetic in tone and in which she professed her desire to cooperate with

the investigator's teacher inquiry.

17. The investigator first met with Ms. Allyn on February 8, 2012 to discuss the investigated District teacher. Ms. Allyn was asked to provide copies of e-mail files and other files maintained on the District's computer system by the teacher who was being investigated. To access the teacher's e-mail account, Ms. Allyn referred to a computer file containing employee passwords, and then used the employee's password to access his e-mails. During this process, Ms. Allyn joked about being "Big Brother" with regard to her duties in the District and her abilities to access employee e-mail accounts. Ms. Allyn explained to the investigator that she was able to look at an employee's e-mail and then mark the e-mail as "unread" so that it did not appear to have been opened and previously viewed.

18. During the February 8, 2012 meeting with the investigator, Ms. Allyn attempted to provide an Internet access report for the investigated teacher from the District's Internet filter. That report failed and Ms. Allyn later re-created the report and e-mailed it to the investigator on February 9, 2012. Consistent with the events of February 8, 2012 and the investigator's request, the District's GroupWise logs that show that on February 8, 2012, Ms. Allyn accessed the investigated teacher's e-mail account. This demonstrates that Ms. Allyn is well-aware of how to access another employee's e-mail account.

19. During the February 8, 2012 meeting, Ms. Allyn told the investigator that all of the Network's passwords were complex strings of characters including upper and lower case characters, numbers, and special characters. Ms. Allyn also maintained that the passwords were not written down where they could be easily discovered. In fact, there is no requirement that the passwords contain multiple character types. Ms. Allyn's statements were therefore fraudulent and an attempt to conceal her unauthorized accesses of Ms. Singh and Mr. Forseth's e-mail accounts.

20. Also during this first meeting, Ms. Allyn told the investigator that she performed the hands-on file maintenance to the District's computer network.

21. The investigator met with Ms. Allyn for a second time at or about 10:54 a.m. on February 10, 2012 to discuss the teacher. District Associate Superintendent Ray Proctor also

attended this meeting. During the meeting, Ms. Allyn frequently changed her responses when asked questions about the computer system, its file maintenance, and the back-up protocol used by the District.

22. The investigator met with Ms. Allyn for a third time on February 14, 2012. At this time, Ms. Allyn was confronted with the logs showing the suspect accesses into Mr. Forseth's, Ms. Dales' and Ms. Singh's GroupWise accounts.

23. At the outset, Ms. Allyn denied accessing the e-mail accounts of Ms. Singh, Ms. Dales and Mr. Forseth. Ms. Allyn then gave a wide variety of answers as to why she would be accessing the GroupWise accounts of Ms. Singh, Ms. Dales, and Mr. Forseth. Eventually, Ms. Allyn settled on an explanation that she was performing maintenance and fixing problems for the administrators, which required her to access their accounts. Ms. Allyn's explanations included troubleshooting a problem that Ms. Singh was having with her calendar entries intermittently not showing up in her GroupWise calendar when entered by Pat Dales, correcting a font size on Ms. Dales' e-mail preferences and correcting Eric Forseth's e-mail preferences to send forwarded e-mails containing HTML objects in HTML rather than plain text. Due to the nature of the activities evident on the District's GroupWise logs, Ms. Allyn's explanations are implausible. Ms. Allyn's denial of having authorization to access these e-mail accounts perpetrated a fraud upon the District.

24. The District's logs show that Ms. Allyn was logging into the District network under her own personalized login name and password and was then accessing the e-mails of Ms. Singh (via her secretary Pat Dales) and Mr. Forseth using their personalized login names and passwords. The District's GroupWise logs from February 8, 2012 are attached as Exhibit C. The District's GroupWise logs from February 9, 2012 are attached as Exhibit D. The District's GroupWise logs from February 10, 2012 are attached as Exhibit E.

25. Ms. Allyn was placed on paid administrative leave on February 14, 2012 based upon her unauthorized access of Ms. Singh's, Ms. Dales' and Mr. Forseth's District e-mail accounts.

26. Below are the times and locations at which Ms. Allyn, without authorization,

accessed the e-mails of District administrators:

a. On February 8, 2012 at 6:47 a.m., Elaine Allyn accessed the GroupWise account of Pat Dales and then the GroupWise account of Candace Singh from Ms. Allyn's home IP address of 76.176.206.214. See Exhibit C.

b. On February 8, 2012 at 5:13 p.m., Elaine Allyn accessed the GroupWise account of Pat Dales and then the GroupWise account of Candace Singh from Ms. Allyn's home IP address of 76.176.206.214. See Exhibit C.

c. On February 8, 2012 at 5:54 p.m., Elaine Allyn accessed the GroupWise account of Eric Forseth from Ms. Allyn's home IP address of 76.176.206.214. See Exhibit C.

d. On February 9, 2012 at 6:43 a.m., Elaine Allyn accessed the GroupWise account of Pat Dales and then the GroupWise account of Candace Singh from Ms. Allyn's home IP address of 76.176.206.214. See Exhibit D.

e. On February 9, 2012 at 11:56 a.m., Elaine Allyn accessed the GroupWise account of Pat Dales and then the GroupWise account of Candace Singh from Ms. Allyn's workstation IP address of 10.16.1.42. See Exhibit D.

f. On February 9, 2012 at 1:53 p.m., Elaine Allyn accessed the GroupWise account of Pat Dales and then the GroupWise account of Candace Singh using Ms. Allyn's own network ID and Ms. Dales' GroupWise login. See Exhibit D.

g. On February 9, 2012 at 1:58 p.m., Elaine Allyn accessed the GroupWise account of Eric Forseth using Ms. Allyn's own network ID and Mr. Forseth's GroupWise login. See Exhibit D.

h. On February 9, 2012 at 7:49 p.m., Elaine Allyn accessed the GroupWise account of Pat Dales and then the GroupWise account of Candace Singh from Ms. Allyn's home IP address of 76.176.206.214. See Exhibit D.

i. On February 9, 2012 at 8:00 p.m., Elaine Allyn accessed the GroupWise account of Eric Forseth from Ms. Allyn's home IP address of 76.176.206.214. See Exhibit D.

27. Ms. Allyn accessed the e-mails of District administrators on additional occasions. However, because she caused the District's logs to be overwritten, records of these prior

unauthorized accesses have been deleted.

Deletion of District GroupWise Logs

28. Ms. Elaine Allyn is responsible, as the District's Director of Information Systems, for ensuring that the District's network undergoes a timely and routine back-up of its login information. The information saved by this back-up includes the login name of each person who logs in to the District's network and the District's internet account This back-up saves a record of all login information from the time the last back-up was run until the time of the current back-up. Any information saved from a prior back-up is overwritten and deleted.

29. The District's GroupWise logs were originally programmed to undergo a back-up of its login system every thirty (30) days or 1024 MB. Approximately 5,000 days of GroupWise logs can be stored in 1024 MB of file space.

30. On or about February 7, 2012, when Ms. Allyn was first expected to respond to the investigator, she had instead engaged a consultant to perform maintenance on the District computer system.

31. During the February 8, 2012 meeting, because of the difficulties that Ms. Allyn had explaining the District's computer information retention and back-up process, the investigator told Ms. Allyn that it was critical that no logs, e-mails or files be destroyed until the investigator could review the evidence for his investigation. It was also explained to Ms. Allyn that the biggest concern of the investigator was that logs would be overwritten before the logs could be reviewed by computer experts, or that logs that were backed-up would be similarly overwritten by subsequent back-ups. The investigator and Ms. Allyn discussed the possibility that the GroupWise logs would be maintained for at least seven days, if not 30 days as a default setting. Ms. Allyn expressed an understanding of the problem and assured the investigator that computer files were backed-up on a redundant District server and were also backed-up to a remote location.

32. During the February 10, 2012 meeting, when asked to provide access logs to the network and the GroupWise application, Ms. Allyn could not provide any logs relating to the operation of the network and could only find three days of the District's GroupWise logs. When

asked why there were not more GroupWise logs, Ms. Allyn responded that she thought it probably had something to do with the consultant who she had engaged to work on the District network earlier in the week, on February 7, 2012.

33. Ms. Allyn commented that the consultant had "bounced" (rebooted) the server and that may have destroyed the other logs. When asked if the logs might be available on the back-up Ms. Allyn was uncertain.

34. Ms. Allyn advised that the consultant had been engaged to enable GroupWise users to be able to empty their trash mailboxes, a problem that Ms. Allyn claimed was causing the District's GroupWise server's hard drive to fill to dangerously-high levels. Yet, because approximately 5,000 days of District GroupWise logs can be saved in 1024 MB, only a small amount of memory space is needed to save one week of this District GroupWise logs. Thus, Ms. Allyn's excuses are simply an attempt to evade detection of her deceitful activities.

35. Thereafter, a network computer expert began a number of exercises to research potential vulnerabilities in the District's computer system.

36. The network computer expert also reviewed the GroupWise logs provided by Ms. Allyn. These logs were determined to contain entries from February 8, 9, and 10, 2012, up until the time of the second interview of Ms. Allyn at approximately 10:54 a.m. on February 10, 2012. These logs are attached as Exhibits C, D and E.

37. During the third interview on February 14, 2012, Ms. Allyn admitted that after she talked with the investigator on February 10, 2012, she set the retention period of the GroupWise logs to one day.

38. Later it was determined from the District's remote back-up vendor that the retention or overwrite period for items deleted from the GroupWise server had indeed recently been changed to one day and 1024 KB. Thus, all records regarding who was assessing the District's network, internet and e-mails was only saved one day at a time and any previous information was not maintained. This meant that when Ms. Allyn changed these settings, the District's GroupWise logs were overwritten each day, thus destroying information from prior days. Because of Ms. Allyn's actions, all information regarding who was logging into the

District system prior to February 8, 2010 was destroyed.

39. Each back-up resulted in the loss of information stored prior to the time before the previous back-up was run. For example, when a back-up was run every day, only one day of login information was stored in the District's logs. Therefore, when Ms. Allyn changed the schedule for the back-up of the District's logs, she deleted all records of her previous accesses of Ms. Singh's and Mr. Forseth's e-mails and, thus, destroyed evidence of her unlawful behavior.

Deletion of District E-mails

40. As the District's Director of Information Systems, Ms. Allyn was also responsible for ensuring the security and back-up of the District's GroupWise e-mail system. This allows the District to retain copies of all District e-mails.

41. In the summer of 2011, the GroupWise server backed-up District e-mails to a separate back-up server located at the District. These back-ups were kept for three years.

42. The GroupWise application was originally set not to allow the emptying of employee e-mail trash mailboxes until the files were backed-up on the District's back-up server. Some GroupWise server files, including the in and out mailboxes, as well as the trash mailbox were also backed-up to a remote location, a LAN Solutions server using the LAN Vault software.

43. In the fall of 2011, the District set the retention of these e-mails to one year.

44. During the February 8, 2012 meeting, the investigator told Ms. Allyn that it was critical that no logs, e-mails or files be destroyed until the investigator could review the evidence for his investigation. Ms. Allyn expressed an understanding of the problem and assured the investigator that computer files were backed-up on a redundant District server, were also backed-up to a remote location and assured the investigator that those files would be intact.

45. Thereafter, Ms. Allyn disconnected the District's back-up server but continued to back-up some of the GroupWise files to the remote location.

46. After Ms. Allyn was put on administrative leave from the District, it was discovered that Ms. Allyn had changed the LAN Vault settings to overwrite the e-mail trash files one day after the trash was emptied by the user. This essentially gave any message deleted by

a user and emptied from the user's trash a one day back-up rather than one year. This was a further attempt by Ms. Allyn to conceal her wrongful and deceitful acts.

47. In order to hide the evidence of her unauthorized access of the GroupWise e-mail accounts of District administrators, Ms. Allyn willfully destroyed the records of her dishonest activities. Ms. Allyn destroyed or ordered the destruction of the following:

a. On or about February 7, 2012, Elaine Allyn directed computer consultant John Hurst to change the retention settings of the District's GroupWise application to empty the trash receptacles of the GroupWise users' accounts, thereby destroying thousands of e-mail messages.

b. On or about February 7, 2012, Elaine Allyn destroyed GroupWise logs for GroupWise transactions recorded prior to that time.

c. On or about February 10, 2012, Elaine Allyn changed the settings for the retention of GroupWise logs from retaining logs for seven days to retaining logs for one day. This caused further loss of GroupWise logs.

d. On or about February 10, 2012, Elaine Allyn changed the settings in the District's LAN Vault (off-site back-up software) to retain items removed from GroupWise trash receptacles for one day before overwriting the back-up files. This would only provide the District a one-day back-up of deleted e-mail messages, rather than the one-year back-up that was expected.

48. Ms. Allyn took affirmative steps to destroy evidence that she had been hacking into and reading the e-mails of Ms. Singh and Mr. Forseth.

Mishandling of District E-rate Program

49. Ms. Allyn also mishandled the District's E-rate program. Ms. Allyn failed to comply with the District's contracting procedures in her selection of contractors that would be receiving payment under the E-rate program and falsely certified to the Federal Communications Commission (FCC) that she was in compliance with District and FCC requirements. A March 13, 2012 letter from the Universal Service Administrative Company (USAC), requesting additional information to approve the District's 2011-2012 E-rate funding request is attached as

Exhibit F. A full and complete copy of Ms. Allyn's District file for the District's 2011-2012 E-rate program is attached as Exhibit G.

50. In particular, in E-rate funding year 2010-2011, Ms. Allyn failed to seek multiple bids where required, failed to maintain her bid and contracting records for the specified amount of time, and failed to maintain an arms length relationship between the District and its contractor by allowing the contractor to write the specifications for the work to be done. See Exhibit G.

51. Ms. Allyn's actions and inaction have jeopardized a large sum of federal funding for the District. See Exhibits F and G.

52. Ms. Allyn's hacking into the e-mail accounts of District administrators, lying about accessing these accounts, willfully destroying evidence of her wrongdoing and mishandling of the District's E-rate program clearly demonstrate her dishonesty, immoral conduct, misuse of district property, violations of district policies and procedures and failure to comply with the schools laws of the state and federal government. As the District's Director of Information Systems, Ms. Allyn used her position to access the private e-mails of District administrators. She also failed to comply with federal E-rate program requirements, which has jeopardized large amounts of federal funding for the District. Her willful failure to act in a professional and ethical manner has eviscerated the District's trust in Ms. Allyn's ability to discharge her duties in a manner consistent with District expectations, and the requirements of the District Board Policies and Administrative Regulations.

On the basis of the foregoing, I recommend that the Governing Board notify Ms. Allyn of the District's intention to dismiss her as a classified employee of the District for her violations of District Board Policy 4218.

Within 10 calendar days after receiving this recommendation, Ms. Allyn may appeal orally or in writing by signing and filing the card or paper included with the recommendation. Any other written document signed and appropriately filed within the specified time limit by the employee shall constitute a sufficient notice of appeal.

A written notice of appeal is filed only by delivering the notice of appeal to the office of the Superintendent or designee during normal work hours of that office. A notice of appeal may

be mailed to the office of the Superintendent or designee but must be received or postmarked no later than the time limit stated herein.

In cases where an order of suspension without pay has been issued in conjunction with a recommendation of dismissal, any appeal of the recommendation of dismissal shall also constitute an appeal of the suspension order, and the necessity of the order shall be an issue in the appeal hearing.

If Ms. Allyn fails to file a notice of appeal within the time specified in these rules, she shall be deemed to have waived her right to appeal, and the Board may order the recommended personnel action into effect immediately.

I verify that this statement is true of my own knowledge, except as to those matters of which I do not have direct knowledge, and as to those matters, I am informed and believe them to be true.

Dated: April 12, 2012

By: _____
Dennis Bixler
Assistant Superintendent, Human Resources
Fallbrook Union Elementary School District