AR 4040 Tuesday, February 02, 2010 5:04:44 PM

From: prblack@ausdk12.org
To: mstephenson@ausdk12.org
Cc: lhornada@ausdk12.org; hcarver@ausdk12.org

Here's some suggested rewording of the new articles in AR 4040. Sorry I'm getting this to you so late. I can clarify my thinking at the meeting.

AR4040(a)

1.

a. Substitute teachers, non-school employees, and students (including student aides, office helpers, computer lab assistants, and so forth) are not to use teacher workstations except to run specific programs specified by the Superintendent or his/her designee.

b. Each employee's user ID and password are issued to ensure the security and integrity of the network and to keep unauthorized persons from accessing confidential data. Employees will safeguard their user ID and password at all times and take every precaution to ensure that they are not compromised. Employees will not use anyone else's user ID and will not share their user ID and password with anyone else, including student aides and assistants.

2.

a. To prevent unauthorized persons from seeing or accessing information, when employees leave a classroom or office for any reason or for any period of time, no matter how short, their computer workstation is to be locked so that their password is required to unlock it, or it is to be turned off completely. It is not sufficient to turn off the monitor or minimize all windows.

b. Employees must be aware that computer viruses can be passed from one computer to another through infected media, such as disks, CDs, DVDs, or flash drives. Employees are to exercise caution before reading data or files from any sort of media or over the network, and should consult with technical staff if they have any doubt or question about the integrity or safety of such a data transfer.

c. Because submitting an email address to a non-work related site, replying to "spam" (email containing solicitations from an unknown or untrusted source), clicking on links in spam, downloading attachments in unsolicited email, or clicking on a pop-up advertisement can make their workstation vulnerable to malicious software and encourage the receipt of more spam, employees will avoid such actions. If unsure about the safety of any email message or action, they should consult with technical staff before taking any action.

Thanks,
Paul

Paul Black
Albany USD Board of Education
prblack@ausdk12.org
(510) 589-9576
http://www.PRBlack.com/BoE