STAFF USE OF PERSONAL COMMUNICATION DEVICES

Use of personal communication devices ("PCDs") (as defined in Bylaw 0100) has become pervasive in the workplace. For purposes of this policy, "personal communication device" includes computers, tablets (e.g., iPad-likes ~~and similar~~ devices), electronic readers ("e-readers"; e.g., Kindle-likes ~~and similar~~ devices), cell phones ~~(e.g., mobile/cellular telephones~~, smartphones ~~[~~(e.g., ~~BlackBerry,~~ iPhones, Android devices, Windows Mobile devices~~]~~). and/or other web-enabled devices of any type. Whether the PCD is Board-owned and assigned to a specific employee, or personally-owned by the employee (regardless of whether the Board pays the employee an allowance for his/her use of the device, the Board reimburses the employee on a per use basis for their business-related use of his/her PCD, or the employee receives no remuneration for his/her use of a personally-owned PCD), the employee is responsible for using the device in a safe and appropriate manner.

Safe and Appropriate Use of Personal Communication Devices, Including Cell Phones/Smartphones

Using a cell phone or other PCD while operating a vehicle is strongly discouraged. Employees should plan their work accordingly so that calls are placed, text messages/instant messages/e-mails read and/or sent, GPS-navigation destinations set/modified, and/or the Internet browsed either prior to traveling or while on rest breaks. In the interest of safety for both Board employees and other drivers, employees are required to comply with all applicable laws while driving (including any laws that prohibit texting or using a cell phone or other PCD while driving).

Employees may not use a PCD in a way that might reasonably create in the mind of another person an impression of being threatened, humiliated, harassed, embarrassed or intimidated.

Duty to Maintain Confidentiality of Student Personally Identifiable Information - Public and Student Record Requirements

Employees are subject to all applicable policies and guidelines pertaining to protection of the security, integrity and availability of the data stored on their PCDs.

Cellular and wireless communications, including calls, text messages, instant messages, and e-mails sent from PCDs, may not be secure. Therefore, employees should use discretion in relaying confidential information, particularly as it relates to students.

Additionally, cellular/wireless communications, including text messages, instant messages and e-mails sent and/or received by a public employee or school official using his/her PCD may constitute public records if the content of the message concerns District business, or an education record if the content includes personally identifiable information about a student. Cellular/wireless communications that are public records are subject to retention and disclosure, upon request, in accordance with Policy 8310 – Public Records. Cellular/wireless communications that are student records should be maintained pursuant to Policy 8330 – Students Records. Finally, cellular/wireless communications and other electronically stored information (ESI) stored on the staff member's PCD may be subject to a Litigation Hold pursuant to Policy 8315 – Information Management. Staff are required to comply with District requests to produce copies of cellular/wireless communications in their possession that are either public records or education records, or that constitute ESI that is subject to a Litigation Hold.

At the conclusion of an individual's employment (whether through resignation, nonrenewal, or termination), the employee is responsible for informing the Superintendent or his/her designee of all public records, student records and ESI subject to a Litigation Hold that is maintained on the employee's Board-owned PCD. The District's IT department/staff will then transfer the records/ESI to an alternative storage device.

If the employee also utilized a personally-owned PCD for work-related communications, and the device contains public records, ~~students~~students' records and/or ESI subject to a Litigation Hold, the employee must transfer the records/ESI to the District's custody (e.g., server, alternative storage device) prior to the conclusion of his/her employment. The District's IT department/staff is available to assist in this process. Once all public records, student records and ESI subject to a Litigation Hold are transferred to the District's custody, the employee is required to delete the records/ESI from his/her personally-owned PCD. The employee will be required to sign a document confirming that all such records/information has been transferred to the District's custody and deleted from his/her personally–owned PCD before the Board will issue any final compensation that is owed to the employee.

If a PCD is lost, stolen hacked or otherwise subjected to unauthorized access, the employee must immediately notify the Superintendent so a determination can be made as to whether any public records, students records and/or ESI subject to a Litigation Hold has been compromised and/or lost. The Superintendent shall determine whether any security breach notification laws may have application to the situation. Appropriate notifications will be sent unless the records/information stored on the PCD was encrypted.

The Board prohibits employees from maintaining the following types of records and/or information on their PCDs:

A. social security numbers

B. driver's license numbers

C. credit and debit card information

D. financial account numbers

E. student personally identifiable information

F. information required to be kept confidential pursuant to the Americans with Disabilities Act (ADA)

G. personal health information as defined by the Health Insurance Portability and Accountability Act (HIPAA)

If an employee maintains records and/or information on a PCD that is confidential, privileged or otherwise protected by State and/or Federal law, the employee is required to encrypt the records and/or information.

It is suggested that employees lock and password protect their PCDs when not in use.

Employees are responsible for making sure no third parties (including family members) have access to records and/or information, which is maintained on a PCD in their possession, that is confidential, privileged or otherwise protected by State and/or Federal law.

Privacy Issues

Except in emergency situations or as otherwise authorized by the Superintendent or as necessary to fulfill their job responsibilities, employees are prohibited from using PCDs to capture, record and/or transmit the words or sounds (i.e., audio) and/or images (i.e., pictures/video) of any student, staff member or other person in the school or while attending a school-related activity. Using a PCD to capture, record and/or transmit audio and/or pictures/video of an individual without proper consent is considered an invasion of privacy and is not permitted.

PCDs, including but not limited to those with cameras, may not be activated or utilized at any time in any school situation where a reasonable expectation of personal privacy exists. These locations and circumstances include, but are not limited to, classrooms, gymnasiums, locker rooms, shower facilities, rest/bathrooms, and any other areas where students or others may change clothes or be in any stage or degree of disrobing or changing clothes. The Superintendent and building principals are authorized to determine other specific locations and situations where use of a PCD is absolutely prohibited.

Personal Use of PCDs While at Work

Board employees may carry PCDs with them while at work including while operating Board equipment, but are subject to the following restrictions:

A. Excessive use of a PCD for personal business during work hours is considered outside the employee's scope of employment and may result in disciplinary action.

B. Employees are personally and solely responsible for the care and security of their personally-owned PCDs. The Board assumes no responsibility for theft, loss, or damage to, or misuse or unauthorized use of, personally-owned PCDs brought onto its property, or the unauthorized use of such devices.

Potential Disciplinary Action

Violation of this policy may constitute just cause for disciplinary action up to and including termination. Use of a PCD in any manner contrary to local, State or Federal laws may also result in disciplinary action up to and including termination.

~~Adopted 1/21/13~~