Book	Policy Manual
Section	DRAFT POLICIES FOR THE BOARD
Title	Copy of STAFF USE OF PERSONAL COMMUNICATION DEVICES
Code	po7530.02
Status	
Adopted	April 16, 2013
Last Revised	February 18, 2020

7530.02 - **STAFF USE OF PERSONAL COMMUNICATION DEVICES**

Use of personal communication devices ("PCDs") has become pervasive in the workplace. For purposes of this policy, "personal communication device" includes computers, tablets (e.g., iPads and similar devices), electronic readers ("e-readers"; e.g., Kindles and similar devices), cell phones (e.g., mobile/cellular telephones, smartphones [e.g., BlackBerry, iPhone, Android devices, Windows Mobile devices, etc.], and/or other web-enabled devices of any type. Whether the PCD is Corporation-owned and assigned to a specific employee or school official or personally-owned by the employee or school official (regardless of whether the Corporation pays the employee or school official an allowance for his/her use of the device, the Corporation reimburses the employee or school official on a per use basis for their business-related use of his/her PCD, or the employee or school official receives no remuneration for his/her use of a personally-owned PCD), the employee or school official is responsible for using the device in a safe and appropriate manner and in accordance with this policy and its accompanying guidelines, as well as other pertinent Board policies and procedures.

Conducting Corporation Business Using a PCD

Employees and school officials are permitted to use a Corporation-owned and/or personally owned-PCD to make/receive calls, send/receive emails, send/receive texts, send/receive instant messages, that concern Corporation business of any kind.

Employees and school officials are responsible for archiving such communication(s) in accordance with the Corporation's requirements.

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

Employees and school officials whose job responsibilities include ~~**regular or occasional**~~ driving ~~**and who use a PCD for business use are expected to refrain from**~~ **are prohibited from holding or** using their device while ~~**driving**~~ **operating a moving motor vehicle during work duties**. Safety must come before all other concerns. Regardless of the circumstances, including slow or stopped traffic, employees and school officials ~~**should**~~ **shall** pull off to the side of the road and safely stop the vehicle before placing or accepting a call. Reading or sending a text message, instant message or e-mail, or browsing the Internet using a PCD while ~~**driving**~~ **operating a moving motor vehicle** is strictly prohibited. ~~**If acceptance of a call is unavoidable and pulling over is not an option, employees are expected to keep the call short, use hands-free options (e.g., headsets or voice activation) if available, refrain from the discussion of complicated or emotional topics, and keep their eyes on the road. Special care should be taken in situations where there is traffic, inclement weather, or the employee or school official is driving in an unfamiliar area.**~~ **Exceptions to these prohibitions are to place a call to 911 to report a bona fide emergency or using the telecommunications device with hands-free or voice-activated technology. In cases of reporting a bona fide emergency, if possible, the driver should move to the side of the road and stop the vehicle before using the cell phone, electronic device, mobile phone, or telecommunications device.** In the interest of safety for employees, school officials, and other drivers, employees and school officials are required to comply with all applicable State laws and local ordinances while driving, including any laws that prohibit texting or **holding/**using a cell phone or other PCD while driving.

Employees and school officials 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 and school officials are subject to all applicable policies and guidelines pertaining to protection of the security, integrity and availability of the data stored on a PCD regardless of whether they are Corporation-owned and assigned to a specific employee

or school official or personally-owned by the employee or school official.

PCD communications, including calls, text messages, instant messages, and e-mails sent or received may not be secure. Therefore, employees and school officials should use discretion when using a PCD to relay confidential information, particularly as it relates to students.

Additionally, PCD 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.

Further, PCD communications about students, including text messages, instant messages and e-mails sent and/or received by a Corporation employee or school official using his/her PCD may constitute education records if the content includes personally identifiable information about a student.

Communications, including text messages, instant messages and e-mails sent and/or received by a Corporation employee or school official using his/her PCD, that are public records or student records are subject to retention and disclosure, upon request, in accordance with Policy 8310 – Public Records. PCD communications that are student records should be maintained pursuant to Policy 8330 – Students Records.

It is the responsibility of the Corporation employee or school official who uses a PCD for Corporation business-related use to archive all text messages, instant messages and e-mails sent and/or received using his/her PCD in accordance with the Corporation's requirements.

Finally, PCD communications and other electronically stored information (ESI) stored on the staff member's or school official's PCD may be subject to a Litigation Hold pursuant to Policy 8315 – Information Management. Employees and school officials are required to comply with Corporation requests to produce copies of PCD 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 or official service (whether through resignation, nonrenewal, or termination), the employee or school official 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 or school official's Corporation-owned PCD. The Corporation's IT department/staff will then transfer the records/ESI to an alternative storage device.

If the employee or school official utilized a personally-owned PCD for Corporation-related communications, and the device contains public records, students records and/or ESI subject to a Litigation Hold, the employee or school official must transfer the records/ESI to the Corporation's custody (e.g., server, alternative storage device) prior to the conclusion of his/her employment or official service. The Corporation'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 Corporation's custody, the employee or school official is required to delete the records/ESI from his/her personally-owned PCD.

If a PCD is lost, stolen, hacked or otherwise subjected to unauthorized access, the employee or school official must notify the Superintendent immediately so a determination can be made as to whether any public records, student records and/or ESI subject to a Litigation Hold have been compromised and/or lost. Pursuant to Policy 8305 Information Security and its accompanying guidelines, 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 were encrypted.

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

Corporation employees may carry PCDs and/or cell phones with them while at work, but are subject to the following restrictions:

A. Excessive use of a PCD or cell phone 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 Corporation property, or the unauthorized use of such devices.

Potential Disciplinary Action

Violation of any provision 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 also may result in disciplinary action up to and including termination.

Revised 8/21/18

Legal	Protecting Children in the 21st Century Act, Pub. L. No. 110-385, Title II, Stat. 4096 (2008)
	Children's Internet Protection Act (CIPA), Pub. L. No. 106-554 (2001)
	20 U.S.C. 1232g
	34 CFR Part 99