Policy

STAFF AND SCHOOL OFFICIALS USE OF PERSONAL COMMUNICATION DEVICES

Use of personal communication devices ("PCDs") (as defined in bylaw 0100) has become pervasive in the workplace. Whether the PCD is Board-owned and assigned to a specific employee or school official, or personally-owned by the employee or school official (regardless of whether the Board pays the employee an allowance for their use of the device, the Board reimburses the employee or school official on a per use basis for their business-related use of their PCD, or the employee or school official receives no remuneration for their 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 guideline, as well as other pertinent Board policies and guidelines.

Conduction District Business Using a PCD

Employees and school officials are permitted to use a Board-owned and/or personally owned PCD to make/receive calls, send/receive digital communication, that concern District business of any kind.

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

Employees and school officials who receive District business-related communication(s) on Board-owned and personally-owned PCDs on a function that is not permitted under this policy are still responsible for the following:

A. Archiving such communication(s) sent or received in accordance with the District's requirements; and
B. Responding to an individual who sends such communication using the employee's or school official's District-issued digital communication account with the following message; "On _____ (insert date), I received a message from you on my ____Board-owned ____ personally-owned PCD. Pursuant to Board Policy 7530.01, please contact me with such communications regarding District business of any kind via my personal communication device, the District issued digital communication account from which I am sending this message. Thank you."

Safe and Appropriate Use of a PCD

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 using their device while driving. Safety must come before all other concerns. Regardless of the circumstances, including slow or stopped traffic, employees and school officials should pull off to the side of the road and safely stop the vehicle before placing or accepting a call. Reading or sending a digital communication or browsing the Internet using a PCD while driving is a violation of State law and 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 complicate 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 is driving in an unfamiliar area. 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 digital communication or using a cell phone or other PCD while driving).

In situations where job responsibilities include regular driving and accepting of business calls, the employee or school official should use hands-free equipment to facilitate the provisions of this policy.

Employee 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 Board-owned and assigned to a specific employee or personally-owned by the employee.

PCD communications, including calls, digital communication sent or received may not be secure. Therefore, employees should use discretion when using a PCD to relay confidential information, particularly as it relates to students.

Additionally, PCD communications including digital communication sent and/or received by a public employee or school official using a PCD may constitute public records.

Further, PCD communications about students, including digital communication sent and/or received by a District employee or school official using their PCD may constitute education records if the content includes personally identifiable information about a student.

Communications, including digital communication sent and/or received by a District employee or school official using their PCD, that are public records or student 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 – Student Records.

It is the responsibility of the District employee or school official who uses a PCD for District business-related use to archive all digital communication sent and/or received using their PCD in accordance with the District's requirements.

Cellular/Wireless communications and other electronically stored information (ESI) stored on the staff member's or school officials PCD may be subject to a litigation hold pursuant to the Wisconsin Records Retention laws. Staff and school officials 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 District Administrator or their designee or 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 District related communications, and the device contains public records, students' records, and/or ESI subject to 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 their 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 their 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 their personally-owned PCD.

If a PCD is lost, stolen, hacked, or otherwise subjected to unauthorized access, the employee or school official must immediately notify the District Administrator, so a determination can be made as to whether any public records, student records, and/or ESI subject to a litigation hold has been compromised and/or lost. Pursuant to Policy #7540 – Staff Technology Acceptable Use and Safety. The District Administrator 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 and school officials from maintaining the following types of student, staff, or District records and/or information on their PCD:

A. Social Security numbers
B. Driver's license numbers
C. Credit and debit card information

It is recommended 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 an emergency situation or as otherwise authorized by the District Administrator 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 District Administrator and building principals are authorized to determine other specific locations and situations where use of a PCD is absolutely prohibited.

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 may also result in disciplinary action up to and including termination.

NEOLA 2023

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. 123g
34 C.F.R. Part 99