Book	Policy Manual
Section	7000 Property
Title	Phase IV Technology Update - January 2018 Revised ACCESS TO DISTRICT TECHNOLOGY RESOURCES AND/OR INFORMATION RESOURCES FROM PERSONAL COMMUNICATION DEVICES
Number	*po7542 EAR
Status	
Adopted	December 10, 2009
Last Revised	May 14, 2018

7542 - **ACCESS TO DISTRICT TECHNOLOGY RESOURCES AND/OR INFORMATION RESOURCES FROM PERSONAL COMMUNICATION DEVICES**

For purposes of this policy, "personal communication device" (PCD) includes computers, tablets (e.g., iPad-like devices), electronic readers ("e-readers"; e.g., Kindle-like devices), cell phones, smartphones (e.g., iPhones, Android devices, Windows Mobile devices, etc.), ~~( )~~ ~~telephone paging devices (e.g., beepers or pagers)~~, [NOTE: END OF OPTION] and/or other web-enabled devices of any type.

[X] The Board of Education provides both a guest network and business network. The business network is a secure network for the conduct of official District business. Access to the business network requires prior approval and authorization by the District. The guest network is a CIPA-compliant non-secured network provided for use by students, parents, and other visitors while on school property. Only Board-approved communication devices and authorized users may access the business network. Any non-Board-approved communication devices or non-authorized users must be pre-approved by the Superintendent.

[X] [OPTION #1]

The Board of Education prohibits individuals from using their ~~personal communication devices (~~PCDs~~)~~ to access ~~the~~ District~~'s technology resources (e.g., networks, servers, projectors, printers, etc.)~~ Technology and/or Information Resources (as defined in Bylaw 0100) while on-site at a District facility. ~~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.)), **( )** telephone paging devices (e.g., beepers or pagers), **( )** and/or other web-enabled devices of any type.~~

[x-] Exceptions to this policy must be approved in advance, in writing, by the Superintendent.

[END OF OPTION #1]

[X] [OPTION #2]

The Board of Education permits

- **( )** employees,
- **( )** students,
- **( )** Board members,
- **( )** guests,
  - **( )** , as well as
    - **( )** contractors,
    - **( )** vendors,
    - **( )** agents,

to use their ~~personal communication devices (~~"PCDs"~~)~~ to wirelessly access the District's ~~technology resources (guest or business networks, servers, projectors, printers, etc.)~~ Technology and/or Information Resources (as defined in Bylaw 0100) while they are on-site at any District facility. **( )** Access to the business/guest network shall require authentication.

~~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 phone (e.g., mobile/cellular telephones, smartphones (e.g., BlackBerry, iPhone, etc.), **( )** and/or other web-enabled devices of any type.~~

[ ] If the user wants to access the ~~District's technology resources~~ District's Technology and/or Information Resources through a hard-wired connection, the user's PCD must first be checked by the _____ to verify it meets the established standards for equipment used to access the network.

The District Technology Coordinator~~_____~~ **(X~~ -~~)** is charged with developing or, **( )** is directed to develop the necessary standards for connecting PCDs to the District's Technology and Information Resources~~technology resources~~. The standards shall be available upon request.

The standards shall be designed and enforced to minimize the Board's exposure to damages, including, but not limited to, the loss of Confidential ~~sensitive District data~~ Data/Information, illegal access to Confidential Data/Information~~confidential data,~~ damage to the District's intellectual property, damage to the District's public image/reputation, and damage to the District's critical internal systems, from unauthorized use.

The use of PCDs must be consistent with the established standards for appropriate use as defined in Policy 7540.03 and AG 7540.03 - Student ~~Education~~ Technology Acceptable Use and Safety, Policy 7540.04 and AG 7540.04 - Staff ~~Education~~ Technology Acceptable Use and Safety, Policy 5136 and AG 5136 - Personal Communication Devices, Policy 7530.02 - Staff Use of Personal Communication Devices. When an individual connects to and uses the District's ~~technology resources~~ Technology and/or Information Resources, s/he must agree to abide by all applicable policies, administrative guidelines and laws (e.g., the user will be presented with a "splash screen" that will set forth the terms and conditions under which s/he will be able to access the District's Technology and/or Information Resource(s)~~technology resource(s);~~ the user will need to accept the stated terms and conditions before being provided with access to the specified technology resource(s)).

In order to comply with the Children's Internet Protection Act ("CIPA"), the Board has implemented technology protection measures that protect against (e.g., filter or block") access to visual displays/depictions/materials that are obscene, constitute child pornography, and/or are harmful to minors. The Board also utilizes software and/or hardware to monitor online activity to restrict access to child pornography and other material that is obscene, objectionable, inappropriate and/or harmful to minors.

Any user who violates the established standards and/or the Board's Acceptable Use policy, or who accesses the District's Technology and/Information Resources~~technology resources~~ without authorization may be prospectively denied access to the District's Technology and/or Information Resources~~technology resources~~. If the violation is committed by a contractor, vendor or agent of the District, the contract may be subject to cancellation. Further disciplinary action may be taken if the violation is committed by a student or employee.

The owner of a PCD bears all responsibility and assumes all risk of theft, loss, or damage to, or misuse or unauthorized use of the device while it is on Board property. This provision applies to everyone, regardless of their affiliation or connection to the District.

[END OF OPTION #2]

Last Modified by Beth Rutledge on May 14, 2018