REPLACEMENT POLICY - VOL. 31, NO. 1

ACCESS TO DISTRICT TECHNOLOGY RESOURCES FROM PERSONAL COMMUNICATION DEVICES

The Board permits employees, students, Board members, guests, as well as contractors, vendors, and agents,to use their personal communication devices ("PCDs") to wirelessly access the internet while they are on-site at any 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 phone (e.g., mobile/cellular telephones, smartphones (e.g., BlackBerry, iPhone, etc.), and/or other web enabled devices of any type.

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 Network and Internet Acceptable Use and Safety, Policy 7540.04 and AG 7540.04 – Staff Network and Internet Acceptable Use and Safety, Policy 5136 and AG 5136 - Personal Communication Device, Policy 7530.02 - Staff Use of Communication Devices. When an individual connects to and uses the District's technology 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 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 resources without authorization may be prospectively denied access to the District's 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.

Deleted: NETWORK ACCESS FROM PERSONALLY-OWNED COMPUTERS ¶ AND/OR OTHER WEB-ENABLED DEVICES¶

Formatted: Indent: Left: 0", First line: 0"

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.

Adopted 11/16/09

Deleted: Board members, District employees, and students, as well as other approved persons, contractors, vendors, and agents, may use their personal computers or web-enabled devices of any type to access the District's server and internal network while they are on-site at any District facility, provided the computers and web-enabled devices meets the established standards for equipment used to access said server and network, and the individual granted access complies, without exception, with the established standards for appropriate use of the District's server and network.¶
¶
Connecting to the District's server and network shall be in accordance with standards established by the District. Access to the standards for connecting to the District's server and network using a personal computer or web-enabled device of any sort shall be provided upon request for all to whom this policy applies.¶
¶
Establishment, and subsequent enforcement, of the standards is intended to minimize the District's potential exposure to damages, including, but not limited to, the loss of sensitive District data, illegal access to confidential data, damage to the District's intellectual property, damage to the District's public image, and damage to the District's critical internal systems, from unauthorized use.¶
¶
Any Board member, employee, student, contractor, vendor, or agent of the District who violates the established standards, who violates the District's Acceptable Use policy, or who accesses the server and network without authorization may be subject to disciplinary action, up to and including expulsion, if a student, termination of employment if a District employee, denial of access if a Board member, or cancellation of the contract with the District if a contractor, vendor or agent. Further, the Board member, employee, student, contractor, vendor, or agent ... [1]

Board members, District employees, and students, as well as other approved persons, contractors, vendors, and agents, may use their personal computers or web-enabled devices of any type to access the District's server and internal network while they are on-site at any District facility, provided the computers and web-enabled devices meets the established standards for equipment used to access said server and network, and the individual granted access complies, without exception, with the established standards for appropriate use of the District's server and network.

Connecting to the District's server and network shall be in accordance with standards established by the District. Access to the standards for connecting to the District's server and network using a personal computer or web-enabled device of any sort shall be provided upon request for all to whom this policy applies.

Establishment, and subsequent enforcement, of the standards is intended to minimize the District's potential exposure to damages, including, but not limited to, the loss of sensitive District data, illegal access to confidential data, damage to the District's intellectual property, damage to the District's public image, and damage to the District's critical internal systems, from unauthorized use.

Any Board member, employee, student, contractor, vendor, or agent of the District who violates the established standards, who violates the District's Acceptable Use policy, or who accesses the server and network without authorization may be subject to disciplinary action, up to and including expulsion, if a student, termination of employment if a District employee, denial of access if a Board member, or cancellation of the contract with the District if a contractor, vendor or agent. Further, the Board member, employee, student, contractor, vendor, or agent of the District who violates the established standards or who violates the District's Acceptable Use policy may be denied access to the District's server and network in the future.