ACCEPTABLE USE OF PERSONAL PORTABLE ELECTRONIC DEVICES

The District's computer network is provided for staff and students to enhance the educational programs of the District; to further District goals and objectives; and to conduct research and communicate with others. In addition, the District recognizes the value of using Personal Portable Electronic Devices ("PPED") in conjunction with the computer network. PPED include such items as cell phones; personal digital assistants (PDAs); netbooks; laptops; tablets; iPads; iPods; jump drives/USB drives; flash drives; keychain drives; disk-on keys; MP3 players; and other devices with wireless network cards or cellular network capability.

PPED serve as both communication tools as well as instruments of learning. PPED may be used for approved educational purposes and/or incidental personal use on school property and/or at District events, subject to the standards in this policy as well as guidelines established at the building level.

While the Board recognizes the proper, appropriate use of PPED by District employees and students, it seeks to prevent their use in ways that disrupt the educational environment of the school or jeopardize the safety, health, and well-being of employees and students. The use of PPED creates the potential for disruption to the academic environment, testing/examination security, and violations of privacy.

This policy is to be read in conjunction with applicable law and existing District policies and regulations including but not limited to the District's Computer Network for Education Policy (No. 4526), the Internet Safety Policy (4526.1), and the Code of Conduct (5300). This policy supplements rather than supplants existing policies; as such, the same standards of acceptable student and/or employee conduct set forth under those policies apply to the use of PPED by students and employees.

Regardless of where or when PPED are used, communications between District employees and students on such devices must always be appropriate and professional in terms of content, time, and frequency. Such communications must be for educational purposes and/or to relay information associated with athletic, extracurricular or other school activities.

In addition to the policies and guidelines as set forth above, the following apply:

Student Use

a) Students may not use PPED in the classroom unless specifically authorized by the instructor.

b) Students may not use PPED during any test, examination or in any situation with the potential for plagiarism or cheating.

c) PPED may not be used in any bathroom, locker room or other areas where individuals have an expectation of privacy.

Staff Use

a) Staff shall not use PPED during times when they are to be performing their job duties unless relevant and necessary thereto.

b) PPED may not be used in any bathroom, locker room or other areas where individuals have an expectation of privacy.

ACCEPTABLE USE OF PERSONAL PORTABLE ELECTRONIC DEVICES

No Privacy Guarantee

Data files and e-mail used in conjunction with the District's computer network shall remain District property, even if stored and/or maintained on PPED. Such data and e-mail are subject to District control and inspection. The District Superintendent or his/her designee may access all such files and communications without prior notice to ensure system integrity and that users are complying with requirements of District policy and accompanying regulations. Staff and students should not expect that information stored on the District's computer network, even if accessed via PPED, will be private.

Guidelines for Acceptable Use of PPEDs

It is not the intention of this policy to define all appropriate usage of PPEDs. Acceptable uses of PPEDs include, but are not limited to, the following:

1. Staff members members are permitted to connect PPEDs to the District's wireless network for usage which shall be limited to school-related issues or activities. Access to some resources via PPED may not be available.

2. Staff shall be responsible for all set-up and configuration of their PPED to connect to a secured guest wireless network.

3. Staff shall be responsible for all support for their PPED. Staff is responsible for resolving any technical problems related to the use of PPED in connection with guest access to District computer resources. District technical staff will not provide assistance, evaluate, or be obligated to support any PPED.

4. Staff shall understand that all Internet access on a PPED connected to the DCS District's wireless network is filtered and monitored using the dDistrict's standard web-filtering software.

5. Users of PPEDs shall abide by all other District policies on the use of computerized and network resources.

6. Staff will accept that PPEDs are the responsibility of the owner. The District shall assume no liability for the theft or damage to a PPED.

7. Staff should exercise common sense and ensure that personal information is protected when using PPEDs in the school.

Prohibitions

It is not the intention of this regulation to define all inappropriate usage. However, in addition to the general requirements of acceptable staff behavior, activities which shall be prohibited by staff and students using PPEDs in conjunction with the computer network include, but are not limited to, the following:

1) Using PPEDs in any way which that results in unauthorized charges or expense to the District.

ACCEPTABLE USE OF PERSONAL PORTABLE ELECTRONIC DEVICES

2) Using PPEDs in a way that damages, disables or otherwise interferes with the operation of District computers, computer systems, software or related equipment through physical action or by electronic means; such as connecting PPED devices directly or indirectly to District hardware or District wired network resources, including but not limited to wired network jacks, printers, interactive whiteboards, or any other District-owned computer/ or electronic resources or peripherals.

3) Using PPEDs itn a way that installs any unauthorized software on the District's computer network.

4) Using PPEDs for changing, copying, renaming, deleting, reading or otherwise accessing files or software not created by the staff member or student without express permission.

5) Using PPEDs to violate copyright law, including the illegal use or sharing of copyrighted music, videos, software or other works of creative expression.

6) Using PPEDs to employ the District's computer network for commercial purposes, proselytizing for religious causes, or political lobbying.

7) Disclosing an individual's password to others or using others' passwords to access District wireless resources via a PPED.

8) Using a PPED to share confidential student or employee information without authorization.

9) Sending or displaying offensive or obscene messages or pictures via a PPED.

10) Harassing, insulting, bullying, threatening or attacking others via a PPED.

11) Engaging in practices that threaten the function and integrity of the computer network.

12) Violating regulations prescribed by the Ddistrict's network services provider.

13) Use of the District's computer wireless resources for other than authorized school-related work or activities.

14) Use of a PPED's cellular or wireless connection to access pornography, obscenity, or resources harmful to minors.

15) Assisting a student to violate District policy and/or regulation, or failing to report knowledge of student violations of the District's policy and regulation.

16) Use which violates any other aspect of District policy or regulations, or which violates local, state or federal laws.

Any user of the District's computer network that accesses another network or other computer resources shall be subject to that network's acceptable use policy.

ACCEPTABLE USE OF PERSONAL PORTABLE ELECTRONIC DEVICES

Sanctions

The District's Technology Director will report suspected inappropriate behavior to the staff member's supervisor who will take appropriate disciplinary action. Any other reports of inappropriate behavior, violations or complaints will be routed to the staff member's supervisor for appropriate action. Violations may result in a loss of access to the District's computer network and/or disciplinary action in accordance with application collective bargaining agreements. When applicable, law enforcement agencies may be notified.

Notification

All staff will be provided a copy of the District's policies on staff and student use of computerized information resources and the regulations established in connection with those policies. Each staff member will sign Technology Use Form before establishing an account or for continuing their use of the District's computer network after a change of assignment.

Adopted: April 18, 2012
Reaffirmed: April 8, 2015