COMPUTER/INTERNET ACCEPTABLE USE POLICY

(Also in the 16-17 Student Handbook & Code of Conduct – Section 11)

A student's use of the District's computers and Internet resources is a privilege, not a right. Student-users of the District's computer network and Internet access are expected to use this technology as an educational resource.

Student computer network/Internet users are expected to behave responsibly in accessing and viewing information that is pertinent to the educational mission of the District. Students are required to abide by the generally accepted rules of network etiquette. These include, but are not limited to the following:

1. **Use of Appropriate Language.** The District's Internet system has been established for an educational purpose. As such, the District prohibits student users from using language which is inconsistent with an educational purpose. The use of the following type of language is prohibited:

    a. Criminal speech and speech used in the course of committing a crime (for example: threats to the President or to any other person, instructions on breaking into computer systems, child pornography, drug dealing, purchase of alcohol, gang activities, etc.);

    b. Speech that is inappropriate in the educational setting or violates District rules (such as obscene, profane, lewd, vulgar, threatening, harassing or discriminatory language or false or defamatory material about a person/organization; dangerous information that if acted upon could cause damage or present a danger of disruption; violations of privacy/revealing personal, private information about others); and

    c. In some circumstances, such as on District-sponsored student Web pages, the District may require that student publications meet a variety of standards related to adequacy of research, spelling and grammar and appropriateness of material (i.e., that school Web pages must relate to school and career preparation activities).

2. Sending, receiving, transferring, viewing, sharing or downloading obscene, pornographic, lewd or otherwise illegal materials, images, videos or photographs, including but not limited to sexually explicit images or images portraying nudity.

2. **Access to Information.** Students are prohibited from accessing the following categories of material or information on the Internet or World Wide Web:

    a. material that is profane or obscene;

    b. material that is pornographic, expressly including child pornography;

    c. material that is harmful to minors (i.e., pictures or visual depictions which, taken as a whole, appeal to a prurient interest in nudity, sex or perverted or lewd acts);

    d. material that advocates or condones the commission of unlawful acts; or

    e. material that advocates or condones violence or discrimination towards other people.

    Students are advised that the District utilizes a Technology Protection Measure that blocks or filters Internet access to the above categories of material/information, as well as other categories of material or information which the District has deemed inappropriate for viewing by students in the educational setting.

3. Online Safety/Privacy: Students are required to complete an Internet safety course. The curriculum will focus on educating students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response. The course content will be prescribed to the building principals by a designated administrator within the District's IT Department at the beginning of each school year. The IT administrator will ensure the content is consistent with federal requirements.

Students are prohibited from giving out personal information for non-educational reasons pertaining to themselves such as: addresses, telephone numbers, parents' work addresses or telephone numbers or the name and location of their school, even through email correspondence unless specifically authorized by the District and with the consent of the students' parents/guardians. Students must tell their teachers and/or parents immediately if they come across information which makes them feel uncomfortable. Students must never agree to get together with someone they "meet" online without first discussing it with their parents. If their parents agree to the meeting, students must ensure that the meeting is in a public place and that they are accompanied by one of their parents.

Only Web 2.0/Social Networking tools and applications, including but not limited to instant messaging, chat rooms, wiki spaces, blogs and other methods of interactive electronic communication, approved by a designated administrator within the IT Department, and aligned to the National Educational Technology Standards for Students (NETS*S) may be utilized for instructional purposes in the attainment of the educational goals of the District. Technology Protection Measures are in place to block or filter Internet access to non-approved Web 2.0 tools and applications. Any digital communications are subject to District review at any time. Technology Protection Measures will be used to red-flag digital communications that violate Pennsylvania or federal law or District policy. Routine maintenance and monitoring of the District's system may lead to discovery that a student has violated the law or a District policy. An individualized search of a student's profile, log files, history, etc., will be conducted if there is reasonable suspicion that a user has violated the law or District policy.

5. Electronic Mail (email): Students may only use email solutions approved by a designated administrator within the IT Department. Students must understand that there is no guarantee of privacy in their email messages and that email messages are subject to District review at any time. Technology Protection Measures will be used to red-flag emails that violate the law or a District policy/rule. Routine maintenance and monitoring of the District's system may lead to discovery that the student has violated the law or a District policy/rule. An individualized search of a student's email will be conducted if there is a reasonable suspicion that a user has violated the law or District policy/rule. Email should be used only for legitimate educational purposes or as authorized by the District. Students should be courteous and respectful in their email messages to others. The use of students' email accounts will be permitted for instructional purposes aligned to the National Educational Technology Standards for Students (NETS*S) and for the attainment of the District's educational goals.

6. Plagiarism: Students are reminded that it is plagiarism to "cut/copy and paste" information from the Internet and then pass it off as their own original ideas. Students are prohibited from plagiarizing information and resources from the Internet and are reminded to cite proper sources used from the Internet.

7. Copyright Infringement: All communications and information via the network (i.e., the Internet) should be assumed to be private property and protected by copyright. Students may not reproduce copyrighted material without explicit permission of the author/owner. Only public domain software can be downloaded.

8. Unauthorized or Disruptive Use/Hacking: Students are prohibited from using the District network in such a way that would disrupt the use of the network by other users. Students may not create or maliciously distribute computer viruses. Students may not destroy another person's data. Students may not access or attempt to access other computer systems or access files without authorization.

9. Purchase of Products or Services: Students are prohibited from purchasing products or services through the District network. The District is not responsible for any financial obligations arising from unauthorized use of the District network for the purchase of products or services.

10. Student Passwords/Accounts: Students may not share their passwords to anyone nor allow unauthorized network access via their account.

11. Unauthorized Disclosure, Use or Dissemination of Personal Information: Students may not disclose, use or disseminate personal information about students, especially minor students, without the authorization of that student's parent/guardian and without specific authorization from the District.

12. Prohibition on Using Peer-to-Peer Networking Applications: Students are prohibited from using peer-to-peer networking applications on the Internet/World Wide Web.

13. Personal Electronic Communication Devices: Students are permitted to bring their personal electronic communication devices to school and onto the District's network as set forth in the District's Electronic Devices Policy. Personal electronic devices are permitted only on the District's SDCE Wireless network. District users, both students and staff, must use their District computer login credentials in order to connect to the SDCE wireless network. The District's Computer/Internet Acceptable Use Policy and all other District policies apply to the use of personal electronic communication devices. Reconfiguration of device settings may be required to access the District's network.

ELECTRONIC COMMUNICATION DEVICES POLICY
(BRING YOUR OWN DEVICE POLICY- BYOD)

District students and employees are permitted to possess and use District-owned and Personal Electronic Communication Devices, when in compliance with this policy, other district policies, regulations, rules, and procedures, internet service provider ("ISP") terms, and local, state, and federal laws, and when that possession and use is supportive of the educational program of the district. However, the possession and use of District-owned and Personal Electronic Communication Devices by students and employees that are (a) found to be disruptive to the educational process and/or environment or (b) used in ways that negatively affect students, employees, and the district's mission and environment, is prohibited in accordance with this Policy, other district policies (including the district's Acceptable Use Policy), regulations, rules and procedures, ISP terms, and local, state, and federal laws.

1. **Definitions**

a. Electronic Communication Devices - are communication devices with voice, data, text, and/or navigation capabilities that are able to access the Internet, transmit telephone calls, text messages, email messages, instant messages, video communications (such as iChat and Skype), perform word processing and other computer and online applications (apps), and provide location information. The devices are capable of electronically communicating, sending, receiving, storing, recording, reproducing, and/or displaying information and data.

Examples of Electronic Communication Devices include smartphones (iPhone, Android, Blackberry), cellular phones, mobile phones (with recording and/or camera/video and other capabilities and configurations), traditional telephones, pagers, global positional system (GPS) instruments, computers, portable game units, graphic calculators, MP3/music and media players or recorders, personal digital assistants ("PDAs"), traditional cameras, video cameras, digital still cameras, tablet and laptop computers, and other similar devices. Electronic Communication Devices may also be referred to as electronic devices in other publications and district policies.

Electronic Communication Devices also include devices that are not capable of transmitting telephone communications (such as iPads, Android tablets, radios), and devices that may or may not have Internet access (such as Kindles, Nooks, or other eReaders), are lasers, are capable of recording still and video images, are capable of recording audio, and/or are radar communication devices.

b. Personal Electronic Communication Devices - are Electronic Communication Devices that are owned by the student or employee.

2. **Authority**

The Board permits the use of District-owned and Personal Electronic Communication Devices by district students and employees during the school day in district buildings, on district property, and while students are attending district-sponsored activities during regular school hours when they are in compliance with this policy, other district policies, regulations, rules, and procedures and applicable local, state and federal laws, and so long as such use does not interfere with the students' educational requirements, students' or employees' responsibilities/duties and performance, the rights and education of others, and the operation and services of the district.

Students must access the Internet on their Personal Electronic Communication Devices via the district's content-filtered wireless "SDCE" network. The SDCE network is for District users and a user must enter their District login credentials to access the SDCE network. Using any means to bypass the district's filter is strictly prohibited. Students are not permitted to connect to the Internet through 3G/4G/mobile broadband

connections. Failure to comply with this requirement shall result in confiscation of the Personal Electronic Communication Device and loss of privilege to bring/use the Device at school.

Building level administrators, in consultation with the Superintendent and in compliance with this policy, other district policies, regulations, rules, and procedures, are authorized to determine the extent of the use of Personal Electronic Communication Devices within their schools, on the school's property, and while students are attending that school's sponsored activities during regular school hours. For example, use of Personal Electronic Communication Devices at the elementary grade level may be different than that at the middle school, and/or high school grade levels. Teachers shall determine authorized use within their respective classrooms.

Unless a teacher determines otherwise, District-owned and Personal Electronic Communication Devices must be turned off upon entering any instructional area and remain off until the student leaves the instructional area. Instructional areas include, but are not limited to, classrooms, gymnasiums, practice fields, field trip locations, auditoriums, band rooms, and chorus rooms.

The district shall have the right to restrict Personal Electronic Communication Devices during school evacuations, as necessary, for the safety and security of all individuals.

The District shall not be liable for the theft, loss, damage, misuse, or unauthorized use of any Personal Electronic Communication Device brought to school by a student or employee. Students and employees are personally and solely responsible for the security of Personal Electronic Communication Devices brought to school, school events, or district property. The District will not be responsible for restricting, monitoring, or controlling the personal electronic communications of students or employees; however, it reserves the right to do so if the communications traverse the district network.

If Personal Electronic Communication Devices are loaned to or borrowed and/or misused by nonowners, the owners of the Personal Electronic Communication Devices are jointly responsible with the nonowner for the misuse and/or violation of district policy, regulations, rules, or procedures.

3. **Guidelines**

a. In accordance with this policy, District-owned and Personal Electronic Communication Devices **<u>may</u>** be used in authorized areas or as determined by the school administration as follows:

(i) For educational or instructional purposes.

(ii) Before and after school, in the cafeteria at lunchtime, in the hallways during the passing of classes, on the district's bus if authorized by the bus driver, and in the library and a study hall if authorized by the teacher.

(iii) When the educational, safety, emergency, medical, or security use of Personal Communication Devices by the student is approved by the building principal, or designee, or the student's IEP team. In such cases, the student's use must be supervised by a district professional.

All use of Personal Electronic Communication Devices shall conform with the district's Acceptable Use Policy and all other applicable district policies and local, Pennsylvania and federal laws.

b. In accordance with this policy, District-owned and Personal Electronic Communication Devices **<u>may not</u>** be used in unauthorized areas or as determined by the school administration within their schools, on the school's property, and while attending that school's sponsored activities during regular school hours as follows:

(i) Students and employees are prohibited from connecting Personal Electronic Communications Devices to the District-owned network or other District-owned devices, via a hard-wired connection. Any permissible access to the District-owned network by Personal Electronic Communications Devices is only available through a wireless connection.

(ii) To access, download, receive, create, send, share, view, sell, purchase or otherwise disseminate obscene, pornographic, lewd or otherwise illegal materials, images, photographs or video content, including but not limited to sexually explicit images or images portraying nudity. **This prohibition shall be strictly enforced and students found to be in violation of this policy provision shall face discipline up to and including expulsion from the District.**

(iii) Students and employees are prohibited from attaching a nondistrict owned wireless access point, wireless router, or wireless bridge to the district owned network.

(iv) Students and employees are prohibited from establishing a "mobile hotspot" or otherwise permitting other users to use their Personal Electronic Communications Device as a technological means to gain access to Internet resources or websites.

(v) Students are STRICTLY prohibited from using District-owned or Personal Electronic Devices to make an audio or video recording of any person, including but not limited to other students or District employees, on school district property, on district-provided transportation or at school-sponsored events unless directed by a teacher to do so as part of an educational assignment and when the individuals being recorded give permission to be recorded.

(vi) Building administrators are authorized to establish authorized student use in their respective buildings. If the building administrator authorizes the use of Personal Electronic Communication Devices in classrooms at any given time, the students' use is then at the discretion of the classroom teacher and such use may be prohibited by the teacher if he/she feels appropriate. Building administrators and teachers may also prohibit the use of Personal Electronic Communication Devices in classrooms and common areas of the school if they are determined to be disruptive to the educational process.

(vii) The Board strictly prohibits the possession by students of any nondistrict-owned laser pointers, or laser pointer attachments, and any Personal Electronic Communication Devices that are hazardous or harmful to students, employees, and the district on school grounds, at district-sponsored activities, and on buses or other vehicles provided by the district. These include, but not limited to, devices that control/interfere with the operation of the buildings' systems, facilities and infrastructure, or network. No exception or permission may be authorized by the principal, or designee, or anyone, for students to possess or use such devices.

(viii) During tests, examinations, and/or assessments, unless the teacher authorizes such use. When Personal Electronic Communication Devices are not permitted to be used during tests, examinations, and/or assessments they must be stored in closed items such as pocketbooks and book bags, and may not be visible or turned on. For example, they may not be placed on the desktop, table or on an individual's lap. Building administrators are authorized to require that Personal Electronic Communication Devices be stored outside of the classroom during certain examinations and/or assessments, such as the PSSAs or Keystone Exams.

(ix) To cheat, engage in unethical conduct, and threaten academic integrity.

(x) Students and staff may not use Personal Electronic Communication Devices (while on school district property or attending school-sponsored activities) to gain access and/or view Internet resources or websites that are blocked by the district's content filter. Examples include, but are not limited to, social media sites and other prohibited content as defined in the district's Acceptable Use Policy. Although many Personal Electronic Communication Devices provide 3G/4G/mobile broadband connections to the Internet, students and staff use of such connections to access Internet resources or websites which are blocked by the district network is prohibited. Although prohibited by this policy, there are no district technology measures available to block such access if such access is made through 3G/4G/mobile broadband connections to the Internet.

(xi) To invade the privacy rights of any student or employee, violate the rights of any student or staff member, or harass, threaten, intimidate, bully or cyberbully any student, employee, or guest, or promote or engage in violence. Actions include, but are not limited to, taking an individual's photo without consent, recording an individual's voice or image without consent, or storing/accessing personal and/or academic information/data without consent.

(xii) In locker rooms, bathrooms, dressing rooms, and swimming pool areas and in the school nurse office.

(xiii) To create, send, share, view, or disseminate sexually explicit, lewd images or video content.

(xiv) To disrupt the educational and learning environment.

c. A student's use of a District-owned or his/her Personal Electronic Communication Device that violates this Policy, other relevant district policies, regulations, rules, and procedures and/or in a manner that is inconsistent with the instructions or directives given by any district official shall be confiscated and returned only to the student's parent or legal guardian.

d. If a student refuses to comply with a request by a District official/employee to hand over his/her District-owned or personal electronic communication device, that student shall have committed an act of "insubordination" within the meaning of the District's Student Handbook.

e. If school officials have reasonable suspicion that this Policy, other relevant district policies, regulations, rules, procedures, and laws are violated by the student's use of District-owned or Personal Electronic Communication Devices and/or that the use of these devices materially and substantially disrupt the school's atmosphere, the devices may be lawfully searched in accordance with applicable law, and/or the Personal Electronic Communication Devices may be turned over to law enforcement, when warranted. The scope of the search shall be limited to finding evidence of the specific suspicion of a violation of rules, policies or laws. **School officials shall contact the Superintendent or his/her designee prior to searching any Personal Electronic Communication Device.** By using Personal Electronic Communication Devices on school property, students and employees consent to their being searched for evidence of violations of District policies regarding technology and network use. Employees and students not willing to submit their devices for such examination are prohibited from bringing them onto school property and should not do so.

f. Students and employees should have no expectation of privacy when using the district's wireless network or other service(s). In addition, students and employees should have no expectation of privacy when they use Personal Electronic Communication Devices on the district's wireless, SDCE network or other service(s).

g. When legally required and/or when in the interest of the student, the student's parent/guardian shall be notified.

h. If a Personal Electronic Communication Device, is suspected of being stolen, it shall be turned over to law enforcement.

i. Disciplinary consequences shall be in accordance with the district's policies, regulations, rules, and procedures, including but not limited to Student Discipline outlined in this Policy, the Student Handbook, Acceptable Use Policy, Bullying and Harassment Policy and any other policies. Students shall be disciplined in a manner consistent with those policies, discipline ranging from detention, suspension up to and including expulsion, depending on the severity of the infraction. Students may be prohibited on a per student basis from bringing their Personal Electronic Devices to school as a result of violations of this policy.

j. School district Information Technology (IT) support staff members are not permitted to perform work on or configure Personal Electronic Communication Devices.

(i) IT support staff members may provide general guidelines on how to wirelessly connect to the district network in accordance with the guidelines in this policy.

(ii) IT support staff members may assist in a lawful investigation of a Personal Electronic Communication Device only when directed by a school district administrator who is responsible for determining the legality of the search.

(iii) IT support staff will assign a lower priority to supporting Personal Electronic Communication Devices versus district-owned and supported network resources. If Personal Electronic Communication Devices are found to adversely impact the performance of the district-owned network, access to the network by those devices may be disabled.

k. Any authorized wireless access to the district-owned network by Personal Electronic Communication Devices will be subject to content filtering and may have a higher level of security measures applied to the connection than would otherwise be the case with a similar district-owned device.

l. Violations of this Policy should be reported to a school district administrator.