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 deem-1(d)-1(e)-1(n)-1(t)M514 arropried fo, 910(i)-5(e)-1(w)4(s)4(o)9(n)]TETQ gq0 0.000018 m

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 c1 Device at school.

(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 enforc.**

(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.

(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.