SCHOOL DISTRICT OF THE CITY OF ERIE

BOARD POLICY

ADULT USE OF TECHNOLOGY RESOURCES

The purpose of the District's computer networking environment is to facilitate communications in support of research and education by providing access to unique resources and opportunities for collaborative work. The Board expects that all administration, faculty and staff will learn to use computers, electronic mail, the Internet and other telecommunications devices ("technology resources"). The Board also expects that they, as well as volunteers and any other adults who access the District's technology resources (collectively, "adult users") will use them in appropriate ways for the performance of tasks associated with their positions and assignments and the District's educational objectives, generally. The Board encourages adult users to make use of technology resources to explore educational topics, conduct research and communicate with others and incorporate best practices with technology for the purposes of improving efficiency and student achievement. .

In accordance with the Children's Internet Protection Act ("CIPA") and the No Child Left Behind Act of 2001, the District will maintain and enforce a technology protection measure with respect to all of its computers having access to technology resources. Such technology protection measure will block or filter access through technology resources to visual depictions that are obscene or contain pornography. In addition, adult users may not utilize technology resources for the unauthorized disclosure, use or dissemination of personal confidential information regarding students or other adult users.

It is the policy of the District to maintain an environment that promotes ethical and responsible conduct by adult users in all uses of its technology resources. Toward this end, the Board directs the Superintendent to specify what behavior will be permitted, and what behavior is prohibited, as well as appropriate procedures to guide adult users' use of the District's technology resources, generally. Adult users are expected to communicate in a professional manner consistent with any and all state and federal laws governing the behavior of school employees as well as intellectual property rights. It shall be a violation of this policy for any adult user to engage in any activity that does not conform to the established purpose, general rules, policies and/or procedures applicable to the use of the District's technology resources.

SCHOOL DISTRICT OF THE CITY OF ERIE

POLICY AND PROCEDURES FOR ADULT USE OF TECHNOLOGY RESOURCES

The School District of the City of Erie ("District") provides technology resources to members of its administration, faculty, staff, volunteers and other adults ("adult users") in order to facilitate communications in support of research and education. The District anticipates that the use of computers, electronic mail, the Internet and other telecommunications devices ("technology resources") will expedite the sharing of effective practices, lessons and other education-related information across the District and will help adult users to stay on the leading edge of education by forming partnerships with others across the nation and around the world. The School District's technology resources are facilitated by the Information Technology Department ("IT Department"). In furtherance of these goals and objectives, it is the policy of the District to maintain an environment that promotes ethical and responsible conduct in the use of technology resources by adult users. Through this and other policies, it is the intent of the District to comply with the provisions of the Children's Internet Protection Act ("CIPA") and the No Child Left Behind Act of 2001.

1. General Expectations for Adult Use of Technology Resources

The District expects adult users to utilize technology resources in a professional and responsible manner. However, with access to computers and people all over the world, it is inevitable that adult users will encounter material that may not be appropriate for the educational environment. The District will attempt to limit the access to such material by maintaining and enforcing a technology protection measure with respect to all of its computers having access to technology resources.

The technology protection measure will, to the greatest extent possible, block or filter access through technology resources to visual depictions that are obscene, contain pornography or are otherwise inappropriate. Adult users should not send or open communications through computers and/or the network that may be harmful to minors. However, because no technology protection measure is effective completely, adult users should be aware that inappropriate materials could be encountered during legitimate research or communications. If inappropriate material is inadvertently encountered, it must be disengaged from immediately and removed from computers and/or the network. If necessary, technical assistance should be obtained to do so.

Adult users may not utilize technology resources for the unauthorized disclosure, use or dissemination of confidential personally identifiable information regarding students or other employees.

The District views any use of its technology resources to access or transmit sexually inappropriate material as behavior which justifies immediate discharge from employment without regard to any mitigating factors. Consequently, it is the policy of the District that even a single instance of computer or internet use by an employee to intentionally access, view, transmit or otherwise manipulate any sexually explicit, pornographic, or obscene material shall result in discharge from employment. No mitigating factors will be considered.

2. Supervision of Students' Use of Technology Resources

Adult users will oversee the use of technology resources by students under their supervision to ensure that students adhere to the District's Computer/Internet Acceptable Use Policy for Students. Consequently, adult users should familiarize themselves with the requirements set forth in that policy.

Notwithstanding the existence of technology protection measures, the breadth of technology resources make it possible that students could access obscene, pornographic or otherwise inappropriate materials. Adult users will monitor student use of technology resources and shall disengage obscene, pornographic or otherwise inappropriate materials immediately and remove them from computer and/or the network. If necessary, technical assistance should be obtained to do so.

3. District Supervision of the Use of Technology Resources

The District has a legal obligation to assure that its technology resources are utilized in a manner consistent with its goal of providing a safe and healthy educational environment for its students. This interest applies equally to student use and adult use of technology resources. Therefore, adult users must understand that the District provides no technology resources for the sending and receiving of personal, private or confidential electronic communications. Designated IT department staff shall have access to all electronic communications and may examine messages to ensure compliance with law and this policy. Electronic mail messages may be subject to subpoena or preservation requirements. Messages and/or activities relating to and in support of illegal activities are prohibited and will be reported to the appropriate authorities. The District reserves the right to monitor the use of technology resources. In addition, the District may, in its sole discretion, seize, monitor and/or examine any of its technology resources at any time in order to ensure compliance with law and this policy. No employee should have any expectation of privacy with respect to any use of the District's technology resources.

4. Security

Security on any computer or network is a high priority, especially when the network involves many users. If an adult user identifies a security problem on a computer and/or the network, he/she should notify an administrator within the IT

department immediately. Adult users should not demonstrate the problem to other users.

Adult users may not disclose their password to anyone. Adult users may not utilize another person's name or password to access the District Network. An Adult user may not access, modify or destroy another person's data. Adult users may not attempt to log on to a computer and/or the network as an IT Department Administrator. Any adult user identified as a security risk or having a history of computer use policy violations with the District's or other computer systems may be denied access to the technology resources.

Adult users may not download or install any commercial software, shareware, or freeware to the District's computers and/or network, unless specifically authorized to do so by a designated Administrator within the IT Department. District computers may be audited and unauthorized or unlicensed software or software applications will be removed, and access to such software applications may be banned.

Adult users must not open electronic mail or other communication from suspicious or unidentified sources. In the event that an adult user receives a communication containing a virus or other self-perpetuating program that is potentially harmful or disruptive to computers and/or the network, the adult user should report the incident immediately to an administrator within the IT department.

5. Prohibited Activities

The use of the District's technology resources is a privilege, not a right. Inappropriate use of technology resources, including any violation of this policy, may result in cancellation or restriction of the privilege and, in the case of District employees, disciplinary action.

The following activities are strictly prohibited on the District's computers and/or network:

1. the use of technology resources for commercial or for-profit purposes;

2. the use of technology resources for political campaigning;

3. the unauthorized use of a computer and/or network account by anyone but the owner of the account;

4. the unauthorized acquisition of information on other users, obtaining of copies of data belonging to other users, modification of files of other users, or acquisition and/or use of passwords belonging to other users;

5. the use of technology resources not in the direct furtherance of the District's educational purposes , including the creation, facilitation and/or

perpetuation of "chain letters", mass emails, or similar forms of broadcast email;

6. the destruction, modification or abuse of computer hardware or software;

7. using the District network in such a way that would disrupt the use of the network by other users. Adult users may not create or maliciously distribute computer viruses. Adult users may not access or attempt to access other computer systems or access files without authorization.

8. the use of profanity or inappropriate language in electronic mail or other network communication;

9. the downloading or uploading of pirated or illegal software in violation of copyright law and/or the reproduction of copyrighted material without the express permission of the author/copyright owner;

10. the use of technology resources to intentionally access, view, transmit or otherwise manipulate or process any sexually explicit, pornographic, suggestive or obscene material, inappropriate text files, or files dangerous to the integrity of a computer and/or the network;

11. the unauthorized disclosure, use, or dissemination of personal or confidential information of students and/or other employees;

12. the use of technology resources by an adult user to give the false impression that he/she represents the District in a given capacity;

13. the transmission of any material in violation of federal or state law.

6. Bring Your Own Device (BYOD)

Adult users are permitted to bring their personal devices onto the District's network. Personal devices are permitted only on 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. The same School District of the City of Erie, policy and procedures for adult use of technology resources apply to the use of personal devices.

7. District Disclaimers of Liability

When utilizing technology resources, there is always the risk of a system failure, which could result in loss of data, interruption of service, etc. The District disclaims any responsibility for losses incurred as a result of system failure and adult users are advised to make a personal back-up of material contained/saved on the District's technology resources.

The District cannot ensure the reliability or accuracy of information maintained on or accessed through the District's technology resources. The District disclaims responsibility for losses incurred as a result of reliance on unreliable or inaccurate information.

The District disclaims responsibility for any misuse or unauthorized use of its technology resources by adult users and disclaims responsibility for any harm caused to the adult users, to other persons or to organizations through misuse or unauthorized use of the District's technology resources as set forth in this policy.

Due to the nature of the vast amount of information and material available on the Internet, it is impossible for the District to completely restrict access to all controversial materials. Accordingly, the District is not responsible for materials acquired or viewed by adult users through the District's technology resources.

The District is not responsible for personal devices used on the District's campus or network.

509209.v2

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.