CENTENNIAL SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE AND DIGITAL TECHNOLOGY

ADOPTED: October 14, 2014

REVISED:

815. ACCEPTABLE USE AND DIGITAL TECHNOLOGY

1. Purpose

24 P.S. Sec. 4604
20 U.S.C. Sec. 6777
47 U.S.C. Sec. 254

Policy Statement

The school district makes various forms of DIGITAL TECHNOLOGY available to its students for educational purposes and to its employees to advance the education of students or to advance the legitimate business of the school district. These and no other purposes are the exclusive purposes that the school district makes DIGITAL TECHNOLOGY available to its students and to its employees.

2. Definitions

The following terms, when set forth in this policy in capital letters, shall have the meaning set forth in the following definitions unless the context clearly indicates otherwise:

COMPUTER(S) shall mean and INCLUDE desktops; workstations; electronic readers or devices in the nature of an iPad; laptops; servers; routers; digital switches; smart phones; PDAs; and any other digital device in the nature of any of the foregoing.

CLOUD APPLICATION shall mean any service or resource available on the Internet INCLUDING such services or resources as virtual servers or any electronic storage that is outside of the school district's firewall, including such things as a Google™ or Google Chrome™ account; My Drive™; Skydrive™; Adobe Creative Cloud™; Dropbox™; Evernote™; and other similar services.

DATA shall mean all forms of digital or electronic DATA, INCLUDING digital or electronic: records; material; DATA; documents; files; script; code; software; and programs.

DIGITAL TECHNOLOGY shall mean all forms of DIGITAL TECHNOLOGY, INCLUDING DATA, software, hardware, the school district's network and all components of the school district's network and digital services of any nature and kind, that is based on DIGITAL TECHNOLOGY and that is owned, leased or licensed to the school district; accessed by or through DIGITAL TECHNOLOGY

	that is owned, leased or licensed to the school district and that is supplied by the school district to students, employees or VISITORS. DIGITAL TECHNOLOGY INCLUDES COMPUTERS; DATA servers; networks; the Internet; cell phones; beepers; PDAs; modems; voicemail; email; chat-rooms; instant messaging; user groups; and such similar technologies. **INCLUDES** and **INCLUDING** shall mean inclusive of but not limited to and/or by way of example and not limitation. **MALICIOUS CODE** shall mean any code in any part of a software system or script that is intended to or that does cause undesired effects, security breaches, degradation to system speed or functionality to or damage to a system; INCLUDING attack scripts, viruses, malware, worms, Trojan horses, backdoors, time bombs, and malicious active content.
SC 1302	**PARENT(S)** shall mean a student's parent, guardian or other person having legal responsibility of or for the student; INCLUDING a resident who has signed an affidavit for a student in accordance with section 1302 of the School Code. **PORNOGRAPHY/CHILD PORNOGRAPHY** or **PORNOGRAPHIC** INCLUDES any visual or audio depiction, INCLUDING any photograph, digital image, film, video, picture, recording or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct; nude pictures or images of the genitalia of any male or female or the breasts of any female, INCLUDING any photograph, digital image, film, video, picture, or computer or computer-generated image or picture of such; and the definition of such terms in any federal or Pennsylvania state statute. **STUDENT RECORD** shall mean any item of information gathered within or outside the DISTRICT that is directly related to an identifiable student. **SUPERINTENDENT** shall mean the Superintendent, or the Acting Superintendent or Interim Superintendent, or the designee of any of them. **USER** shall mean a student, employee or visitor who is using any DIGITAL TECHNOLOGY. **USER ID** shall mean the identification number(s) or letter(s) that is unique and that is assigned to the individual student or employee. **VISITOR(S)** shall mean any person who is granted access to or who obtains access to any portion of the school district's DIGITAL TECHNOLOGY other than students or employees, INCLUDING contractors, vendors, and PARENTS.

3. Guidelines	<u>Prohibitions – Students, Employees and Visitors</u> Students, employees and visitors of the school district shall not: 1. Use any DIGITAL TECHNOLOGY for any purpose other than for the legitimate educational purposes of our students or for purposes of advancing the legitimate business of the school district; 2. Use any DIGITAL TECHNOLOGY for personal business or affairs, except as expressly provided in this policy or in administrative regulations promulgated and adopted by the SUPERINTENDENT; 3. Use any of our COMPUTERS or DATA unless and until a confidential USER ID and password has been assigned to the student or employee; 4. Use any of our COMPUTERS or DATA without using his/her USER ID and password; 5. Terminate use of any COMPUTERS without logging off the COMPUTER; 6. Disclose his/her USER ID or password to any other individual; 7. Use or utilize the USER ID and/or password belonging to or assigned to any other individual, or impersonate, in any manner, any other person; 8. Open or logon to any COMPUTER, software, program or application using, utilizing or inputting the USER ID and/or PASSWORD of any other individual or entity, or use any default or preset USER ID and/or PASSWORD without express authority; 9. Misrepresent his/her identity when using the school district's COMPUTERS; 10. Bypass any blocking or security software that may be used or installed by the school district; 11. Intentionally, willfully, maliciously or through reckless indifference damage or corrupt the functioning of any DIGITAL TECHNOLOGY or any DATA stored, either temporarily or permanently on any DIGITAL TECHNOLOGY; 12. Visit or access pornographic websites, use search engines or services such as Google, Bing, or any other search engine or function to obtain listing of pornographic websites, pornographic pages, or pornographic pictures;

	13. When using the school district's DIGITAL TECHNOLOGY, violate the school district's Code of Student Conduct or any other applicable policy of the school district; 14. Use any COMPUTERS unless and until the individual has signed an acknowledgment in the form prescribed by the school district attesting to the individual's understanding of the rules governing the use of DIGITAL TECHNOLOGY. 15. Take possession of any COMPUTER unless or until the individual has signed an agreement in the form prescribed by the school district setting forth the terms and conditions under which the individual is permitted and authorized to have possession of the COMPUTER; 16. Intentionally enter or hack into any secure or confidential area of the school district's systems, network(s) or COMPUTERS without proper authority; hack into any hardware and/or software owned or licensed by the school district for any purpose; use any DIGITAL TECHNOLOGY to hack into anyone else's COMPUTERS or networks in any way or manner that is not authorized;
17 U.S.C. Sec. 101 et seq	17. Violate any copyright laws or the ownership or license rights of any person or entity; 18. Violate the terms or conditions of any license owned by the school district; 19. Violate the legal rights of others; 20. Knowingly or willfully infect any COMPUTER with any virus; 21. Knowingly or willfully place any MALICIOUS CODE in any COMPUTER, software, or network or network component; plant any virus, MALICIOUS CODE, pornography/child pornography or other prohibited content or software on anyone's COMPUTER, INCLUDING the school district's network or COMPUTER(S), or any component of the school district's network; 22. Use any software or Internet site in violation of any applicable licensing agreement or applicable terms of use; 23. Use any DIGITAL TECHNOLOGY to hack into anyone else's COMPUTERS or networks in any way or manner that is not authorized; 24. Use any DATA mining, robots, or similar DATA gathering and extraction methods in violation of any person's or entity's rights;

18 Pa. C.S.A. Sec. 5701 et seq, 7601 et seq	25. Use DIGITAL TECHNOLOGY to violate any applicable law, INCLUDING the Wiretap and Electronic Surveillance Control Act; violate any applicable criminal statute pertaining to computers, property or electronic devices, INCLUDING Chapter 76 of the Crimes Code, relating to computer offenses; 26. Install any software program onto or in or download any software program onto or in any COMPUTERS without the express written approval of the SUPERINTENDENT, or insert any removable media into the computer for any purpose without permission and/or except for the following, unless the user has been given certain administrative rights: i. Printer drivers; ii. Adobe® Acrobat® Reader®; iii. Updates to installed programs 27. Fail to report to the school district's technology administrator any time when he/she inadvertently visits or accesses a pornographic site; 28. Violate any applicable work rule when using the school district's DIGITAL TECHNOLOGY; 29. Alter or change the DESKTOP or the look or operation of any shared DESKTOP of any COMPUTER; 30. Alter or change the screen saver, or the look or operation of any screen saver, installed by the school district on any shared computer; delete or remove any program, application, security feature, or virus protection from any school district COMPUTER; 31. Incur any charges or costs of any nature or type to the school district in connection with DIGITAL TECHNOLOGY or your use of DIGITAL TECHNOLOGY; except as specifically and expressly authorized in accordance with applicable procurement requirements established by the school district or by law, or telephone charges by an employee incurred for school district purposes and consistent with the employee's authority; 32. Disconnect any computer from the network without prior explicit direction to do so, except for laptop computers issued with the expectation that they will be disconnected from the network;

33. Disconnect any hardware from any computer without prior explicit direction to do so, except with respect to laptop computers issued with the expectation that they will have hardware, such a printers, connected and disconnected;

34. Access another's COMPUTER for any improper or unlawful purpose, INCLUDING to activate the audio or video functions of the COMPUTER or to search the COMPUTER'S files, documents or codes, without the person's prior permission and authority.

35. Use any device or COMPUTER of any nature or type that has camera, video, movie, or audio recording function in any bathroom, dressing room, locker room, shower room or any other room if used for such purposes at that time.

<u>Additional Prohibitions for Teachers, Teaching Staff, and Employees</u>

In addition to all other prohibitions set forth in this and other school district policies, teachers and members of the teaching staff shall not:

1. Communicate with any school district student using any email account other than the email account provided by the school district on the school district's network;

2. Text message with any student without the prior written approval of the principal and only to the extent authorized by the principal.

3. Communicate with any school district student through social media in a manner that would be consistent with this policy;

4. Provide instruction to students over the Internet without express prior written approval from the Principal of the student for the precise instruction or lesson provided at the approved time frame;

5. Communicate with any school district student while on a disciplinary suspension or an administrative leave without express prior written approval from the Superintendent or the Director of Human Resources;

6. Download or save any STUDENT RECORD on any COMPUTER, network or CLOUD APPLICATION owned, leased or in an account possessed by the employee that is not a COMPUTER or network drive that is owned or leased by the school district.

	Responsibilities of the SUPERINTENDENT The SUPERINTENDENT shall take such action as necessary to promulgate and adopt administrative regulations that are not inconsistent with any applicable law or policy of the school district Board of Directors pertaining to the following: 1. Posting and Dissemination of Policy. 2. Integration into Curriculum and School Program. 3. Training Students and Employees with respect to the permissible uses of DIGITAL TECHNOLOGY. 4. Student Code of Conduct. 5. Updating/Upgrading DIGITAL TECHNOLOGY. 6. Access to and safekeeping of DIGITAL TECHNOLOGY. 7. Enforcement of Policy and Regulations.
24 P.S. Sec. 4604	8. Blocking, Filtering and Monitoring Software. The SUPERINTENDENT shall ensure, at least to the extent required by law, that appropriate software is obtained and utilized to block or filter inappropriate websites from being visited or accessed by students or employees; to monitor, track and report the websites that have been visited or accessed with DIGITAL TECHNOLOGY; to track and report all activity on individual COMPUTERS; to preserve the actual condition of a website when it was accessed; and to restore deleted files. 9. Maintenance and Monitoring of School District Website. The SUPERINTENDENT shall develop administrative regulations detailing the content of the school district's website and the links that are placed on the website.
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	10. Children's Internet Protection Act (CIPA). The SUPERINTENDENT shall ensure compliance with CIPA and shall certify as may be required by law that the School District has an Internet safety policy that includes technology protection measures as required by applicable law. Before adopting this policy, the SUPERINTENDENT must provide reasonable notice and hold at least one public meeting to address the proposal. As may be required by applicable law, the SUPERINTENDENT must ensure that the School District's Internet safety policies must include monitoring the online activities of minors; and as required by the Protecting Children in the 21st Century Act, the school district provides

for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyber bullying awareness and response. The Superintendent shall ensure that the protections provided for in this policy are being implemented, including with regard to the following subjects:

a. Access by minors and students to inappropriate matter on the Internet;

b. The safety and security of minors and students when using electronic mail, chat rooms and other forms of direct electronic communications;

c. Unauthorized access, including so-called "hacking," and other unlawful activities by minors online;

d. Unauthorized disclosure, use, and dissemination of personal information regarding minors; and

e. Measures restricting minors' access to materials harmful to them.

Privacy and Ownership

No employee or student using the school district's DIGITAL TECHNOLOGY shall have any right of privacy or expectation of privacy with respect to anything done on or with said DIGITAL TECHNOLOGY; except with regard to the limitations respecting remote access of laptops.

The DIGITAL TECHNOLOGY belongs to, is licensed to, or accessible through DIGITAL TECHNOLOGY that is owned by or licensed to the school district. The school district retains all rights as an owner or licensee with respect to all DIGITAL TECHNOLOGY that it owns or licenses and has, unless restricted by an express agreement with a third party supplier, the rights of an owner or licensee, INCLUDING the rights to use, transfer, inspect, look in, read or store any such DIGITAL TECHNOLOGY.

The SUPERINTENDENT shall develop administrative regulations pertaining to the review of emails to or from students, parents or employees to ensure compliance with this policy.

Notwithstanding anything herein to the contrary, no employee shall read or examine emails of members of the Board of School Directors except when necessary to comply with or respond to a public records request, a litigation hold requirement, or

an order or subpoena in connection with an administrative or judicial action or after written notice has been provided to the School Board member that his or her email will be reviewed.

The school district owns all intellectual property rights of all work prepared or created by any employee in the course and scope of employment for the school district, INCLUDING copyright, in accordance with the terms, conditions and limitations of applicable law. Consequently, no student, employee or visitor may violate the copyright or other intellectual property rights of the school district or deprive by any means or manner the school district's rights with respect to such material.

Permissible and Impermissible Uses of DIGITAL TECHNOLOGY

Students -

DIGITAL TECHNOLOGY may be used only for legitimate educational purposes and in a manner that complies with all rules and prohibitions contained in this Policy or in other applicable policies.

DIGITAL TECHNOLOGY is being provided or made available to students solely as part of the educational program; for the purpose of teaching students how to use and employ DIGITAL TECHNOLOGY; and to further the teaching of the school district's curriculum and educational programs. The school district is not, through DIGITAL TECHNOLOGY that is being made available by the school district to students, creating a public forum, an open public forum or a limited public forum.

DIGITAL TECHNOLOGY may not be used by students for speech or expressive conduct:

1. That materially and substantially interferes with the education process;

2. That threatens immediate harm to the welfare of the school community, or to any individual;

3. That is lewd, vulgar, indecent or obscene or which contains sexual innuendo, metaphor or simile;

4. That encourages unlawful activity;

5. That interferes with another individual's rights;

SC 1303.1-A Pol. 249	6. That constitutes bullying or cyber bullying in violation of school district policy or the Code of Student Conduct; 7. That violates any applicable Policy of the school district; 8. That constitutes liable, slander or defamation; or 9. That is sexually, racially or ethnically related; that is offensive, threatening or an affront to the sensibilities of others, and that is unlawful under the standards of the anti-discrimination laws of the United States. All expressive conduct or material—whether verbal, written, or graphic—created, downloaded, maintained, copied, pasted, harvested or otherwise obtained, used or transmitted by, to, from or with the school district's DIGITAL TECHNOLOGY, is required to be related to the adopted curriculum, assigned classroom activities, or school programs, such as the development of writing skills, the learning of legal, moral and ethical restrictions imposed upon speech and the acceptance of criticism. Consequently, all expressive conduct by students shall be age appropriate; consistent with the rules of grammar, spelling, sentence structure and format being taught by the school district; and consistent with the abilities of the student. No program, software, application or patch may be installed or placed in any school district COMPUTER that is not licensed to and in the name of the school district or that is not authorized in writing to be installed or placed in any school district COMPUTER. Students shall not use DIGITAL TECHNOLOGY provided by the school district for any purpose not connected with the educational program of the school district. This prohibition INCLUDES any of the prohibitions set forth in this Policy or in the Code of Student Conduct; gambling; accessing social network sites unless such access is specifically in accordance with a school district assignment; accessing any site for the purpose of defeating any of the prohibitions in this Policy. *Employees* - The components of the school district's DIGITAL TECHNOLOGY may only be used in a way which is consistent with the intended purpose of the DIGITAL TECHNOLOGY. DIGITAL TECHNOLOGY may only be used to further the curriculum or programs of the school district.

Notwithstanding anything herein to the contrary, during such times as the employee has no work duties, the employee may use DIGITAL TECHNOLOGY to access his or her private or personal Email account from which Email may be sent or received through that account and not through any such an account of the school district. No employee shall violate any of the provisions of this policy or of applicable law when accessing his or her private email account either during the work day or through the school district's DIGITAL TECHNOLOGY. Any email account provided by the school district shall be used only for advancing the interests of the curriculum or school programs, activities or functions.

Communication by employees reflects on the school district. Consequently, expressive activity through DIGITAL TECHNOLOGY shall exhibit an effort at using good grammar, proper style, and good spelling.

No program, software, application or patch may be installed or placed in any school district COMPUTER that is not licensed to and in the name of the school district or that is not authorized in writing to be installed or placed in any school district COMPUTER.

Employees shall not use DIGITAL TECHNOLOGY provided by the school district for any purpose not connected with the educational program of the school district. This prohibition INCLUDES any of the prohibitions set forth in this Policy or in any other applicable policy or administrative regulations of the school district; gambling; accessing social network sites unless such access is specifically in accordance with a school district assignment; accessing any site for the purpose of defeating any of the prohibitions in this Policy.

Employees shall not save, store or transfer any records, material, DATA, documents or files on any DIGITAL TECHNOLOGY that does not belong to the school district or that is not licensed to the school district. Employees using DIGITAL TECHNOLOGY to create, save or store student or school district DATA must create, save or store such DATA on school district's DIGITAL TECHNOLOGY.

Employees shall not cause email to be diverted to or intercepted from the school district's email system to an email or technology system not belonging to or licensed by the school district.

Unless an employee has granted consent otherwise, the email of the employee may not be automatically intercepted and redirected to another employee or person.

Special Rules Pertaining to Social Network Sites

As per policy, employees shall not use social network sites with or to communicate with any student or PARENT of the school district. All use of DIGITAL TECHNOLOGY for school district or work purposes must be on school district's DIGITAL TECHNOLOGY.

As per policy, no supervisor or management level employee shall communicate with any subordinate employee, whether the subordinate employee is or is not directly supervised by the supervisor through any social network site.

Special Rules Pertaining to Laptops or Other DIGITAL TECHNOLOGY Given to Students or Employees to Take Home

In addition to all of the rules set forth in this policy or the Code of Student Conduct:

1. The Superintendent shall provide notification to PARENTS and students as to the students eligible to be issued a laptop.

2. As a condition of the receipt of the laptop or other DIGITAL TECHNOLOGY, both the student and the PARENT must sign an agreement in a form created by the school district setting forth the obligations of the student and PARENT with regard to the care, use and possession of the laptop.

3. No employee or other person shall remotely access a student's laptop or other DIGITAL TECHNOLOGY except for the following purposes and subject to the following terms and conditions exclusively:

    a. Resolution of a Technical Problem. In some instances it may be necessary for a technology employee to access the laptop remotely to resolve a technical problem. If this is needed, the permission of the student or parent must be obtained before remote access is effectuated and must be properly documented. If permission for remote access is given, a permanent record of the approval must be logged, setting forth pertinent information, INCLUDING the time, date, duration of remote access, and reason for remote access.

    b. Remote Software Maintenance. Remote software maintenance means the automatic downloading and configuration changes of software or settings when a student or employee connects to the school district's network. This is permitted without obtaining any additional permission from a student, employee or PARENT.

c. Voluntary Participation in Web-conferences or Other Web-based Activities. Participation in a web-conference or other web-based activity shall constitute the participant's agreement to access to the participant's COMPUTER and all components of same for all incidents associated with the conference or activity. No person engaging in such activity shall perform any function or activity not fairly or properly associated with the conference or web-based activity.

d. Remote Search of Files, Documents, Pictures, Videos, Code or Software on Laptop. No employee or other person may search a laptop remotely unless a remote search is reasonably necessary; the person is specifically authorized to conduct such a search; and the person has a reasonable suspicion that the student or employee is violating applicable laws or policies or rules and that evidence of same can be found on the COMPUTER or that the COMPUTER contains contraband. Where such reasonable suspicion exists, the scope of the search must be reasonably related to the violations that justified the search.

e. Video and Audio. No person may activate the audio or video functions of a laptop remotely except in the following specific circumstances:

   i. The functions are part of an online class or assignment.

   ii. After a laptop is reported lost or stolen in writing on a form developed by the school district for this purpose by the employee or student to whom the COMPUTER has been issued.

<u>Provision of DIGITAL TECHNOLOGY Services</u>

<u>Students</u>: in accordance with the programs in which they are enrolled, shall be provided with only the following DIGITAL TECHNOLOGY services:

1. Access to the Internet, access to software as provided from time-to-time by the school district, digital files from which to access or save work and print servers, subject to the policies, limitations, exclusions and conditions established by the school district.

Employees: as designated by the SUPERINTENDENT, shall be provided with only the following DIGITAL TECHNOLOGY services:

1. Access to the Internet, Email, access to software as provided from time-to-time by the school district, digital files from which to access or save work, and print servers, subject to the policies, limitations, exclusions and conditions established by the school district.

Visitors: visitors who may access the school district's wireless networks in accordance with the terms, conditions and limitations of this Policy and applicable administrative regulations, shall not have any other access to school district DIGITAL TECHNOLOGY. Any such visitor must accept and agree upon all terms and conditions of use as set forth in the Policy, administrative regulations and/or agreement.

No digital services shall be provided by the school district to other individuals or outside companies, entities or suppliers.

Disclaimer of Liability/Disclaimer of Warranties

The school district disclaims all liability and warranties, INCLUDING the following:

1. There are no warranties, express or implied, by operation of law or otherwise, regarding or relating to the DIGITAL TECHNOLOGY provided by the school district to any student, employee, visitor or other person or entity. The school district specifically disclaims all implied warranties, INCLUDING those of merchantability and fitness for a particular purpose.

2. No representations or other affirmation of fact, INCLUDING statements regarding capacity, suitability for use, or performance shall be deemed to be a warranty by the school district for any purpose or give rise to any liability of the school district whatsoever.

3. The school district shall not be liable for any lost or stolen digital or electronic DATA, files, documents or material of any kind that any student, employee or visitor prepares, creates, stores on, sends to, saves to, copies to, or otherwise uses in connection with the school district's DIGITAL TECHNOLOGY or any component thereof.

Discipline

Pol. 218, 317

Students and employees shall be subject to appropriate discipline, including dismissal in the case of employees, and permanent expulsion in the case of students, in the event that any one or more provisions of this policy is violated.

Complaint Procedure

Pol. 103, 104, 248, 249, 348

If any employee, student, or other person has any complaint of any nature or type pertaining to DIGITAL TECHNOLOGY, the uses of DIGITAL TECHNOLOGY at the school district or on its website, INCLUDING complaints or concerns about sexual harassment (*see also*, school district's Sexual Harassment Policy), bullying, cyber bullying (*see also,* school district's Bullying Policy and Code of Student Conduct), racial intimidation, discrimination, or ethnic intimidation, a complaint may be filed with the SUPERINTENDENT, who shall promptly cause the complaint to be properly investigated with the advice or assistance of the solicitor.

DIGITAL TECHNOLOGY Personnel

The school district may, from time-to-time, employ individuals to create, set up and/or maintain one or more forms of DIGITAL TECHNOLOGY. These individuals may be employees of the school district or independent contractors retained for discreet services. All contracts with independent contractors must be reviewed by and approved by the solicitor and Board of School Directors.

DIGITAL TECHNOLOGY Personnel, whether employed solely to create, set up or maintain DIGITAL TECHNOLOGY or employed to create or maintain DIGITAL TECHNOLOGY as an adjunct to other duties:

1. Shall execute an appropriate non-compete and confidentiality agreement, as developed by the solicitor, so that the individual does not compete with the school district in the use, sale or distribution of any DIGITAL TECHNOLOGY which the employee was involved in creating or developing for the school district; does not disclose any confidential information; and use any confidential information for his or her personal benefit;

2. Shall not access any document, DATA, file or information stored in or accessible through the school district's DIGITAL TECHNOLOGY unless access to such document, DATA, file or information is necessary for the individual employee to perform his/her duties as set forth in his or her written job description or to create or maintain any DIGITAL TECHNOLGY in accordance with his or her written job description.

Notwithstanding anything in this Policy to the contrary, DIGITAL TECHNOLOGY personnel shall have such authority as is necessary to enable each to perform his or her specific job duties as set forth in writing in his/her job description.

The SUPERINTENDENT shall review the job description of the head of the school district's technology department no less frequently than annually and shall make such changes or adjustments to the job description as may be necessary or desirable.

Nothing in this policy shall be construed nor is intended to prohibit the school district from providing DIGITAL TECHNOLOGY or services related to DIGITAL TECHNOLOGY to others pursuant to contracts or other arrangements.

References:

School Code – 24 P.S. Sec. 1303.1-A, 1302

PA Crimes Code – 18 Pa. C.S.A. Sec. 5903, 6312, 7601 et seq

Wiretap and Electronic Surveillance Act – 18 Pa. C.S.A. Sec. 5701 et seq

Child Internet Protection Act – 24 P.S. Sec. 4601 et seq.

U.S. Copyright Law – 17 U.S.C. Sec. 101 et seq.

Sexual Exploitation and Other Abuse of Children – 18 U.S.C. Sec. 2256

Enhancing Education Through Technology Act – 20 U.S.C. Sec. 6777

Internet Safety, Children's Internet Protection Act – 47 U.S.C. Sec. 254

Children's Internet Protection Act Certifications, Title 47, Code of Federal Regulations – 47 CFR Sec. 54.520

Board Policy – 103, 103.1, 104, 218, 218.2, 220, 233, 237, 248, 249, 317, 348, 814