KENNETT CONSOLIDATED SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF THE COMPUTER, NETWORK, INTERNET, ELECTRONIC COMMUNICATIONS, AND INFORMATION SYSTEMS

ADOPTED: September 13, 2010

816. ACCEPTABLE USE OF THE COMPUTER, NETWORK, INTERNET, ELECTRONIC COMMUNICATIONS, AND INFORMATION SYSTEMS

TABLE OF CONTENTS

1. Purpose

The Kennett Consolidated School District ("School District") provides employees, students, and Guests ("Users")[1] with hardware, software, access to the School District's Electronic Communications Systems and network, which includes Internet access, whether wired, wireless, virtual, cloud, or by any other means. Guests include but are not limited to visitors, workshop attendees, volunteers, independent contractors, adult education staff, students, board members, vendors, and consultants.

[1] See the Definition section for the defined terms generally provided in initial capital letters through out this Policy.

Computers, network, Internet, Electronic Communications, information systems, databases, files, software, and media (collectively "CIS systems") provide vast, diverse, and unique resources. The Board of School Directors will provide access to the School District's CIS systems for Users if there is a specific School District-related purpose to access information; to research; to collaborate; to facilitate learning and teaching; and to foster the Educational Purpose and mission of the School District.

For Users, the School District's CIS systems must be used for Educational Purposes and performance of School District job duties. Incidental Personal Use (as defined in this Policy) of School District Computers is permitted for employees. Students may only use the CIS systems for Educational Purposes. CIS systems may include School District computers which are located or installed on School District property, at School District events, connected to the School District's network and/or systems, or when using its mobile computing equipment, telecommunication facilities in unprotected areas or environments, directly from home, or indirectly through another Internet service provider ("ISP"), and if relevant, when Users bring and use their own personal Computers or personal electronic devices, and, if relevant, when Users bring and use another entity's Computer or electronic devices to a School District location, event, or connect it to a School District network.

If Users bring personal Computers or personal technology devices onto the School District's property or at School District events or connect them to the School District's network, and systems, and if the School District reasonably believes the personal Computers and personal electronic devices contain School District information or contain information that violates a School District Policy, or the legal rights of the School District or another person, or involves significant harm to the School District or another person, or involves a criminal activity, the personal Computers or personal electronic devices may be legally accessed to insure compliance with this Policy, other School District Policies, regulations, rules, and procedures, ISP terms, and ISP local, state, and federal laws. Users may not use their personal Computers and personal technology devices to access the School District's intranet, Internet, or any other CIS System unless approved by the Technology Manager and/or designee and/or authorized as part of the School District's services for Users.

The School District intends to protect its CIS systems strictly against outside and internal risks and vulnerabilities. Users play a critical role in protecting these important assets and in lessening the risks that can destroy them. Consequently, Users are required to comply fully with this Policy and to report immediately any violations or suspicious activities to the building principals or the Superintendent. Conduct otherwise will result in actions further described in the Consequences for

	Inappropriate, Unauthorized, and Illegal Use section found in the last section of this Policy and provided in other relevant School District Policies, regulations, rules, and procedures.
2. Definitions 18 U.S.C. Sec. 2256(8) 20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254(h)(7)(F)	1. Child Pornography – Under federal law, any Visual Depiction, including any photograph, film, video, picture, or Computer or Computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: a. The production of such Visual Depiction involves the use of a minor engaging in sexually explicit conduct; b. Such Visual Depiction is a digital image, Computer image, or Computer-generated image that is or is indistinguishable from that of a Minor engaging in sexually explicit conduct; or c. Such Visual Depiction has been created, adapted, or modified to appear that an identifiable Minor is engaging in sexually explicit conduct.
18 Pa. C.S.A. Sec. 6312(d) 24 P.S. Sec. 4603	Under Pennsylvania law, any person who intentionally views or knowingly possesses or controls any book, magazine, pamphlet, slide, photograph, film, videotape, Computer depiction, or other material depicting a child under the age of eighteen (18) years engaging in a prohibited Sexual Act or in the simulation of such Act.
18 U.S.C. Sec. 2256(6) 20 U.S.C. Sec. 6777(e)	2. Computer – includes any School District or User provided personal hardware, software, or other technology device used on School District premises or at School District events or connected to the School District network containing School District programs or School District or student data (including images, files, and other information) attached or connected to, installed in, or otherwise used in connection with a Computer. Computer includes but is not limited to the School District's and User's desktop, notebook, powerbook, tablet PC, iPad, Kindle, eBook readers, or laptop Computers, printers, facsimile machine, cables, modems, and other peripherals, specialized electronic equipment used for students' special educational purposes, Global Positioning System (GPS) equipment, RFID, personal digital assistants (PDAs), iPods, MP3 players, thumbdrives, cell phones (with or without Internet access and/or recording and/or camera/video and other capabilities and configurations), telephones, mobile phones, or wireless devices, two-way radios/telephones, beepers, paging devices, laser pointers and attachments, Pulse Pens, and any other such technology developed.

	3. Electronic Communications Systems – any messaging, collaboration, publishing, broadcast, or distribution system that depends on Electronic Communications resources to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print electronic records for purposes of communication across Electronic Communications network systems between or among individuals or groups that is either explicitly denoted as a system for Electronic Communications or is implicitly used for such purposes. Further, an Electronic Communications system means any wire, radio, electromagnetic, photooptical, or photoelectronic facilities for the transmission/transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature, wire or Electronic Communications and any Computer facilities or related electronic equipment for the electronic storage of such communications. Examples include, without limitation, the Internet, intranet, electronic mail services, voice mail services, tweeting, text messaging, instant messaging, GPS, PDAs, facsimile machines, cell phones (with or without Internet access and/or electronic mail and/or recording devices, cameras/video, and other capabilities and configurations). 4. Educational Purpose - includes use of the CIS systems for classroom activities, professional or career development, and to support the School District's curriculum, Policies, regulations, rules, procedures, and mission statement.
20 U.S.C. Sec. 6777(e)(6) 47 U.S.C. Sec. 254(h)(7)(G)	5. Harmful to Minors – under Federal law, any picture, image, graphic image file, or other Visual Depictions that: a. taken as a whole, with respect to Minors, appeals to the prurient interest in nudity, sex, or excretion; b. depicts, describes, or represents in a patently offensive way with respect to what is suitable for Minors, an actual or simulated Sexual Act or Sexual Content, actual or simulated normal or perverted Sexual Acts, or lewd exhibition of the genitals, and c. taken as a whole lacks serious literary, artistic, political, educational, or scientific value as to Minors.
18 Pa. C.S.A. Sec. 5903(e)(6) 24 P.S. Sec. 4603	Under Pennsylvania law, that quality of any depiction or representation, in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it: a. predominantly appeals to the prurient, shameful, or morbid interest of Minors; and

b. is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable for Minors; and

c. taken as a whole, lacks serious literary, artistic, political, educational, or scientific value for Minors.

6. Inappropriate Matter – includes, but is not limited to, visual, graphic, video, text and any other form of indecent, Obscene, pornographic, Child Pornographic, or other material that is Harmful to Minors, sexually explicit, or sexually suggestive. Examples include, taking, disseminating, transferring, or sharing obscene, pornographic, lewd, or otherwise illegal images or photographs, whether by electronic data transfer or otherwise (such as "sexting," e-mailing, texting). Others include, illegal, defamatory, lewd, vulgar, profane, inflammatory, threatening, harassing, discriminatory (as it pertains to race, color, religion, national origin, gender, marital status, age, sexual orientation, political beliefs, receipt of financial aid, or disability), violent, bullying, flagging, terroristic material, or advocating the destruction of property.

7. Incidental Personal Use – incidental personal use of school Computers is permitted for employees so long as such use does not interfere with the employee's job duties and performance, with system operations, or with other system Users as determined by the employee's immediate supervisor in conjunction with the technology manager. Personal use must comply with this Policy, all other applicable School District Policies, regulations, rules and procedures, as well as ISP terms, local, state, and federal laws, and must not damage the School District's CIS systems.

18 Pa. C.S.A. Sec. 5903(e)
18 U.S.C. Sec. 2256
20 U.S.C. Sec. 6777(e)
47 U.S.C. Sec. 254(h)(7)(D)

8. Minor – for purposes of compliance with the federal Children's Internet Protection Act ("FedCIPA"), an individual who has not yet attained the age of seventeen (17). For other purposes, Minor shall mean the age of minority as defined in the relevant law.

18 U.S.C. Sec. 1460
20 U.S.C. Sec. 6777(e)
47 U.S.C. Sec. 254 (h)(7)(E)

9. Obscene – under federal law, analysis of the material meets the following elements:

a. whether the average person, applying contemporary community standards, would find that the material, taken as a whole, appeals to the prurient interest;

	b. whether the work depicts or describes, in a patently offensive way, sexual conduct specifically designed by the applicable state or federal law to be Obscene; and c. whether the work, taken as a whole, lacks serious literary, artistic, political, educational, or scientific value.
18 Pa. C.S.A. Sec. 5903(b) 24 P.S. Sec. 4603	Under Pennsylvania law, analysis of the material meets the following elements: a. the average person, applying contemporary community standards, would find that the subject material, taken as a whole, appeals to the prurient interest; b. the subject matter depicts or describes in a patently offensive way, Sexual Conduct described in the law to be Obscene; and c. the subject matter, taken as a whole, lacks serious literary, artistic, political, educational, or scientific value.
18 Pa. C.S.A. Sec. 5903(e)(3) 18 U.S.C. Sec. 2246 20 U.S.C. Sec. 6777(e) 47 U.S.C. Sec. 254(7)(H)	10. Sexual Act and Sexual Contact – is defined at 18 U.S.C. § 2246(2), at 18 U.S.C. § 2246(3), and 18 Pa. C.S.A. § 5903.
24 P.S. Sec. 4606 47 U.S.C. Sec. 254(h)(7)(I)	11. Technology Protection Measure(s) – A specific technology that blocks or filters Internet access to Visual Depictions that are Obscene, Child Pornography or Harmful to Minors.
18 U.S.C. Sec. 1460(b) 18 U.S.C. Sec. 2256	12. Visual Depictions – includes undeveloped film and videotape and data stored on computer disk or by electronic means which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format, but does not include mere words.
3. Authority SC 510 24 P.S. Sec. 4604 47 U.S.C. Sec. 254(1)	1. Access to the School District's CIS systems through school resources is a privilege, not a right. These systems and resources, as well as User accounts and information, are the property of the School District. The School District reserves the right to deny access to prevent unauthorized, inappropriate, or illegal activity, and may revoke the privilege of access and/or administer appropriate

	disciplinary action. The School District will cooperate to the extent legally required with ISP, local, state, and federal officials in any investigation concerning or related to the misuse of the CIS systems.
	2. It is often necessary to access Users' accounts in order to perform routine maintenance and security tasks. System administrators have the right to access User accounts by interception, including access to stored communication for any reason in order to uphold this Policy, other School District Policies, regulations, rules, and procedures, the law, and to maintain the system. **USERS SHOULD HAVE NO EXPECTATION OF PRIVACY IN ANYTHING THEY CREATE, STORE, SEND, RECEIVE, OR DISPLAY ON OR OVER THE SCHOOL DISTRICT'S CIS SYSTEMS, INCLUDING THEIR PERSONAL FILES OR ANY OF THEIR USE OF THE SCHOOL DISTRICT'S CIS SYSTEMS. The School District reserves the right to record, check, receive, monitor, track, log, access, and otherwise inspect any and all CIS systems use and to monitor and allocate fileserver space.** Users of the School District's CIS systems who transmit or receive communications and information shall be deemed to have consented to having the content of any such communications recorded, checked, received, monitored, tracked, logged, accessed and otherwise inspected or used by the School District, and to having system administrators monitor and allocate fileserver space. Passwords and message delete functions do not restrict the School District's ability or right to access such communications or information.
24 P.S. Sec. 4610 20 U.S.C. Sec. 6777(c)	3. The School District reserves the right to restrict access to any Internet sites or functions it may deem inappropriate through general policy, software blocking, or online server blocking. Specifically, the School District operates and enforces Technology Protection Measure(s) that block or filter online activities of Minors on its Computers used and accessible to adults and students so as to filter or block Inappropriate Matter as defined in this Policy on the Internet. Measures designed to restrict adults' and Minors' access to material Harmful to Minors may be disabled to enable an adult or student (who has provided written consent from a parent or guardian) to access *bona fide* research, not within the prohibitions of this Policy, or for another lawful purpose. No person may have access to material that is illegal under federal or state law.
	4. If a student or an adult is denied access to material in accordance with this Policy, they have the right to submit a claim. An administrator, supervisor, or their designee will expedite a review and resolution of the claim upon receipt of written consent from a parent or guardian of a student and upon the written request from an adult presented to the building principal.

5. The School District has the right, but not the duty, to inspect, review, or retain Electronic Communications created, sent, displayed, received, or stored on or over its CIS systems, to monitor, record, check, track, log, access, or otherwise inspect; and/or to report all aspects of its CIS systems use. This includes any personal Computers, network, Internet, Electronic Communication Systems, Computers, databases, files, software, and media that they bring onto School District property or to School District events that are connected to the School District network, or when using the School District's mobile commuting equipment, telecommunication facilities in unprotected areas or environments, directly from home, or indirectly through another ISP, and if relevant, when Users bring and use another entity's Computer or electronic devices to a School District location, event, or connect it to a School District network and/or systems, and/or that contains School District programs, or School District or other Users' data or information, all pursuant to the law, in order to ensure compliance with this Policy, and other School District Policies, regulations, rules, and procedures, ISP terms, and local, state, and federal laws, to protect the School District's resources, and to comply with the law.

6. The School District reserves the right to restrict or limit usage of lower priority CIS systems and Computer uses when network and computing requirements exceed available capacity according to the following priorities:

   a. Highest – uses that directly support the education of the students.

   b. Medium – uses that indirectly benefit the education of the students.

   c. Lowest – uses that include reasonable and limited educationally related interpersonal communications.

   d. Forbidden – all activities in violation of this Policy, other School District Policies, regulations, rules, and procedures, ISP terms, and local, state, and federal laws.

7. The School District additionally reserves the right to:

   a. Determine which CIS systems' services will be provided through School District resources.

   b. Determine the types of files that may be stored on School District file servers and Computers.

	c. View and monitor network traffic, file server space, processor, and system utilization and all applications provided through the network and Electronic Communications Systems, including e-mail, and other Electronic Communications. d. Remove excess e-mail and other Electronic Communications, or files taking up an inordinate amount of fileserver space after a reasonable time. e. Revoke User privileges, remove User accounts, or refer to legal authorities, and/or School District authorities when violation of this and any other applicable School District Policies, regulations, rules, and procedures occur or ISP terms, or local, state or federal law is violated, including but not limited to those governing network use, copyright, security, privacy, employment, vendor access, data breaches, and destruction of School District resources and equipment. 8. Due to the nature of the Internet as a global network connecting thousands of Computers around the world, Inappropriate Matter can be accessed through the network and Electronic Communications Systems. Because of the nature of the technology that allows the Internet to operate, the School District cannot completely block or filter access to these resources. Accessing these and similar types of resources may be considered an unacceptable use of School District resources and will result in actions explained further in the Consequences for Inappropriate, Unauthorized, and Illegal Use section found in the last Section of this Policy, and as provided in other relevant School District Policies, regulations, rules, and procedures. 9. The School District must publish a current version of the Acceptable Use Policy, and if relevant any accompanying regulations, rules, and procedures, so that all Users are informed of their responsibilities. A copy of this Policy and *the CIS Acknowledgement and Consent Form* must be provided to all Users, who must sign the School District's *CIS Acknowledgement and Consent Form*, either by electronic or written means. 10. Users must be capable and able to use the School District's CIS systems and software relevant to their responsibilities. In addition, Users must agree to the requirements of this Policy, regulations, rules, and procedures.
11. <u>Delegation of Responsibility</u>	1. The Technology Manager, and/or designee, will serve as the coordinator to oversee the School District's CIS systems and will work with other regional or state organizations as necessary to educate Users, approve activities, provide leadership for proper training for all Users in the use of the CIS systems and the

	requirements of this Policy, establish a system to insure adequate supervision of the CIS systems, maintain executed User *CIS Acknowledgement and Consent Forms*, and interpret and enforce this Policy.
Pol. 800	2. The Technology Manager, and/or designee, will establish a process for setting-up individual and class accounts, set quotas for disk usage on the system, establish a Record Retention and Record Destruction Policies and Records Retention Schedule to include electronically stored information and establish the School District virus protection process.
	3. Unless otherwise denied for cause, student access to the CIS systems resources shall be through supervision by the professional staff. Administrators, teachers, and staff have the responsibility to work together to help students develop the skills and judgment required to make effective and appropriate use of the resources. All Users have the responsibility to respect the rights of all other Users within the School District and School District CIS systems, and to abide by the Policies, regulations, rules, and procedures established by the School District, as well as ISP terms, and local, state, and federal laws.
SC 1303.1-A 47 U.S.C. Sec. 254(5)(B)(iii)	4. The building principal and/or designee(s) have the responsibility to educate Minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.
5. <u>Regulations</u>	1. <u>Access to the CIS Systems</u> a. The CIS systems accounts of Users must be used only by authorized owners of the accounts and only for authorized purposes. b. An account will be made available according to a procedure developed by appropriate School District authorities. c. <u>CIS System</u>. This Policy, as well as other relevant School District Policies, regulations, rules, and procedures, ISP terms, and local, state, and federal laws will govern use of the School District's CIS systems for Users. d. Types of Services include, but are not limited to: i. <u>Internet</u>. School District employees, students, and Guests will have access to the Internet through the School District's CIS systems, as needed.

ii. E-Mail. School District employees and others may be assigned individual e-mail accounts for work related use, as needed. Students may be assigned individual e-mail accounts as necessary, by the Technology Manager, and/or designee, and at the recommendation of the teacher who will also supervise the students' use of the e-mail service.

iii. Guest Accounts. Guests may receive an individual account with the approval of the Technology Manager, and/or designee, if there is a specific School District-related purpose requiring such access. Use of the CIS systems by a Guest must be specifically limited to the School District-related purpose and comply with this Policy and all other School District Policies, regulations, rules, and procedures, as well as ISP terms, local, state, and federal laws and may not damage the School District's CIS systems. A School District *CIS Acknowledgement and Consent Form* must be signed in writing or electronically by a Guest, and if the Guest is a Minor a parent's written or electronic signature is required.

iv. Blogs. Employees may be permitted to have School District-sponsored blogs after they receive training and the approval of the School District. All Bloggers must follow the rules provided in this Policy, the School District's Blogging Policy, and other applicable Policies, regulations, rules, and procedures of the School District, as well as ISP terms, and local, state, and federal laws.

v. Web 2.0 Second Generation and Web 3.0 Third Generation Web-based Services. Certain School District authorized Second Generation and Third Generation web-based services, such as blogging, authorized social networking sites, wikis, podcasts, RSS feeds, social software, folksonomies, and interactive collaboration tools that emphasize online participatory learning (where Users share ideas, comment on one another's project, plan or design; implement, advance, or discuss practices and goals; co-create or collaborate) among Users may be permitted by the School District; however, such use must be approved by the Technology Manager, and/or designee, followed by training authorized by the School District. Users must comply with this Policy as well as any other relevant School District Policies, regulations, rules, and procedures, including copyright, participatory learning/collaborative/ social networking, ISP terms, and local, state, and federal laws during such use.

2. Parental Notification and Responsibility

The School District will notify parents/guardians about the School District's CIS systems and the Policies governing their use. This Policy contains restrictions on accessing Inappropriate Matter. There is a wide range of material available on the Internet, some of which may not be fitting with the particular values of the families of the students. It is practically impossible for the School District to monitor and enforce a wide range of social values in student use of the Internet. Further, the School District recognizes that parents/guardians bear primary responsibility for transmitting their particular set of family values to their children. The School District will encourage parents to specify to their child(ren) what material and matter is and is not acceptable for their child(ren) to access through the School's District's CIS system. When out of school, parents are responsible for monitoring their child(ren)'s use of the School District's CIS systems when they are accessing the systems.

3. School District Limitation of Liability

The School District makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the School District's CIS systems will be error-free or without defect. The School District does not warrant the effectiveness of Internet filtering. The electronic information available to Users does not imply endorsement of the content by the School District, nor is the School District responsible for the accuracy or quality of the information obtained through or stored on the CIS systems. The School District will not be responsible for any damage Users may suffer, including but not limited to, information that may be lost, damaged, delayed, misdelivered, or unavailable when using the CIS systems. The School District will not be responsible for material that is retrieved through the Internet, or the consequences that may result from them. The School District will not be responsible for any unauthorized financial obligations, charges, or fees resulting from access to the School District's CIS systems. In no event will the School District be liable to the User for any damages, whether direct, indirect, special, or consequential, arising out the use of the CIS systems.

4. Prohibitions

The use of the School District's CIS systems for illegal, inappropriate, unacceptable, or unethical purposes by Users is prohibited. Such activities engaged in by Users are strictly prohibited and illustrated below. The School District reserves the right to determine if any activity not appearing in the list below constitutes an acceptable or unacceptable use of the CIS systems.

These prohibitions shall be in effect any time School District resources are accessed, whether on School District property, at School District events, connected to the School District's network, when using mobile commuting equipment, telecommunication facilities in unprotected areas or environments, directly from home, or indirectly through another ISP, and if relevant, when a User uses their own equipment.

Students shall be prohibited from visually possessing and using their personal electronic devices or their personal Computers as defined by this Policy, on School District premises and property (including but not limited to buses and other vehicles), at School District events, or through connection to the School District CIS systems, unless expressed permission has been granted by a teacher or administrator, who will then assume the responsibility to supervise the student in the possession and use, or, unless an IEP team determines otherwise, in which case, an employee will supervise the student in its possession and use. Thus, Users are prohibited from using cell phones with or without Internet access and/or recording, and/or camera/video and other capabilities and configurations. Cameras and the like may not be used to take images of others, transfer them, or place them on websites without the consent of Technology Manager, and the person whose photo is being taken. Students who are performing volunteer fire company, ambulance, or rescue squad functions or who need such a personal electronic device or Computer because of their medical condition or the medical condition of a member of the family, with notice and the approval of the school administrator, may qualify for an exemption of this prohibition.

a. <u>General Prohibitions</u>

Except as permitted by this Policy, Users are prohibited from using School District CIS systems to –

i. Communicate about non-work or non-school related communications.

ii. Send, receive, view, download, store, access, print, post, distribute, or transmit material that is Harmful to Minors, indecent, Obscene, pornographic, Child Pornographic, terroristic, sexually explicit, sexually suggestive, including but not limited to, Visual Depictions. Examples include, taking, disseminating, transferring, or sharing Obscene, pornographic, lewd, or otherwise illegal images or photographs, whether by electronic data transfer or otherwise (such as sexting, e-mailing, texting, among others). Neither may Users advocate the destruction of property.

	iii. Send, receive, view, download, store, access, print, distribute, or transmit Inappropriate Matter, as defined in this Policy, and material likely to be offensive or objectionable to recipients.
SC 1301.1-A Pol. 249	iv. Cyberbully another individual or entity (see School District Bullying Policy).
	v. Bully or target a person to make that person a subject of ridicule.
	vi. Access or transmit gambling pools for money, including but not limited to basketball and football, or any other betting or games of chance.
	vii. Participate in discussion or news groups that cover inappropriate and/or objectionable topics or materials, including those that conform to the definition of Inappropriate Matter in this Policy.
	viii. Send terroristic threats, hateful mail, harassing communications, discriminatory remarks, and offensive, profane, or inflammatory communications.
	ix. Participate in unauthorized Internet Relay Chats, newsgroups, instant messaging communications, and Internet voice communications (on-line, real-time conversations) that are not for school-related purposes or required for employees to perform their job duties. Students must obtain consent from their teacher to use IRC's, however they may not use instant messaging or text messaging. Employees may only use instant messaging if consent was obtained from the Technology Manager, and/or designee.
	x. Use in an illegal manner or to facilitate any illegal activity.
	xi. Communicate through e-mail for non-educational purposes or activities. The use of e-mail to mass mail non-educational or non-work related information is expressly prohibited (for example, the use of the "everyone" distribution list, building level distribution lists, or other e-mail distributions lists to offer personal items for sale is prohibited).
	xii. Engage in commercial, for-profit, or any business purposes (except where such activities are otherwise permitted or authorized under applicable School District Policies); conduct unauthorized fund raising or advertising on behalf of the School District and non-school School District organizations; resell School District Computer resources to individuals or organizations; or use the School District's name in any

		unauthorized manner that would reflect negatively on the School District, its employees, or students. "*Commercial purposes"* is defined as offering or providing goods or services or purchasing goods or services for personal use. School District acquisition Policies must be followed for School District purchase of goods or supplies through the School District system.
	xiii.	Engage in political lobbying.
Pol. 814	xiv.	Install, distribute, reproduce, or use copyrighted software on School District Computers or copy School District software to unauthorized Computer systems, intentionally infringing upon the intellectual property rights of others or violating a copyright. See Copyright Infringement section in this Policy, the School District's Copyright Policy, and the School District's Copyright Guidelines Handbook for additional information.
	xv.	Plagiarize works that are found on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as they were one's own.
	xvi.	Install Computer hardware, peripheral devices, network hardware, or system hardware. The authority to install hardware or devices on School District Computers is restricted to the Technology Manager, and/or designee.
	xvii.	Encrypt messages using encryption software that is not authorized by the School District from any access point on School District equipment or School District property. Users must use School District approved encryption to protect the confidentiality of sensitive or critical information in the School District's approved manner.
	xviii.	Access, interfere, possess, or distribute confidential or private information without permission of the School District's administration. An example includes accessing other students' accounts to obtain their grades, or accessing other employees' accounts to obtain information.
	xix.	Violate the privacy or security of electronic information.
	xx.	Send any School District information to another party, except in the ordinary course of business as necessary or appropriate for the advancement of the School District's business or educational interest.

xxi. Send unsolicited commercial electronic mail messages, also known as spam.

xxii. Post personal or professional web pages on the School District's website without administrative approval.

xxiii. Post anonymous messages.

xxiv. Use the name of the "Kennett Consolidated School District" in any form in blogs, emails, on School District Internet pages or websites, on websites not owned by or related to the School District, or in forums/discussion boards, and on social networking websites to express or imply the position of the Kennett Consolidated School District without the expressed, written permission of the Superintendent. When such permission is granted, the posting must state that the statement does not represent the position of the School District.

xxv. Bypass or attempt to bypass Internet filtering software by any method including but not limited to the use of anonymizers/proxies or any websites that mask the content the User is accessing or attempting to access.

xxvi. Advocate illegal drug use, whether expressed or through a latent pro-drug message. This does not include a restriction on political or social commentary on issues, such as the wisdom on the war on drugs or medicinal use.

xxvii. Attempt to or obtain personal information under false pretenses with the intent to defraud another person.

xxviii. Use location devices to harm another person.

xxix. Post false statements.

xxx. Assume the identity of another person.

b. <u>Access and Security Prohibitions</u>

Users must immediately notify the Technology Manager, and/or designee, if they have identified a possible security problem. Users must read, understand, and submit an electronically or written signed *CIS Acknowledgement and Consent Form* and comply with this Policy that includes network, Internet usage, Electronic Communications,

	telecommunications, non-disclosure, and physical and information security Policies. The following activities related to access to the School District's CIS systems, and information are prohibited: i. Misrepresentation (including forgery) of the identity of a sender or source of communication. ii. Acquiring or attempting to acquire passwords of another. Users are required to use unique strong passwords that comply with the School District's password, authentication, and syntax requirements. Users will be held responsible for the result of any misuse of Users' names or passwords while the Users' systems access were left unattended and accessible to others, whether intentional or whether through negligence. iii. Using or attempting to use Computer accounts of others. These actions are illegal, even with consent or if only for the purpose of "browsing." iv. Altering a communication originally received from another person or Computer with the intent to deceive. v. Using School District resources to engage in any illegal act which may threaten the health, safety, or welfare of any person or persons, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal activity, or being involved in a terroristic threat against any person or property. vi. Disabling or circumventing any School District security program or device, for example but not limited to anti-spyware, anti-spam software, and virus protection software or procedures. vii. Transmitting electronic communications anonymously or under an alias unless authorized by the School District. viii. Accessing any website that the School District has filtered or blocked as unauthorized. Examples include, but are not limited to, unauthorized social networking, music download, and gaming sites.
Pol. 830	ix. Users must protect and secure all electronic resources and information, data, and records of the School District from theft and inadvertent disclosure to unauthorized individuals or entities when they are under the supervision and control of the School District, and when they are not under the supervision and control of the School District. Examples include but are not limited to Users working at home, on vacation, or

elsewhere. If any User becomes aware of the release of School District information, data, or records, the release must be reported to the Technology Manager immediately. See the Board's Data Breach Policy for further information.

c. Operational Prohibitions

The following operational activities and behaviors are prohibited:

i. Interference with, infiltration into, or disruption of the CIS systems, network accounts, services, or equipment of others, including but not limited to, the propagation of Computer "worms" and "viruses," Trojan Horse, trapdoor, robot, spider, crawler, and other program code, the sending of electronic chain mail, and the inappropriate sending of "broadcast" messages to large numbers of individuals or hosts. The User may not hack or crack the network or others' Computers, whether by spyware designed to steal information or viruses and worms or other hardware or software designed to damage the CIS systems or any component of the network, or strip or harvest information, or completely take over a person's Computer, or to "look around."

ii. Altering or attempting to alter files, system security software or the systems without authorization.

iii. Unauthorized scanning of the CIS systems for security vulnerabilities.

iv. Attempting to alter any School District computing or networking components (including but not limited to fileservers, bridges, routers, or hubs) without authorization or beyond one's level of authorization.

v. Unauthorized wiring, including attempts to create unauthorized network connections, or any unauthorized extension or re-transmission of any Computer, Electronic Communications Systems, or network services, whether wired, wireless, cable, virtual, cloud, or by other means.

vi. Connecting unauthorized hardware and devices to the CIS systems.

vii. Loading, downloading, or using unauthorized games, programs, files, or other electronic media, including but not limited to downloading unauthorized music files.

viii. Intentionally damaging or destroying the integrity of the School District's electronic information.

ix. Intentionally destroying the School District's Computer hardware or software.

x. Intentionally disrupting the use of the CIS systems.

xi. Damaging the School District's Computers, CIS systems' networking equipment through the Users' negligence or deliberate act, including but not limited to vandalism.

xii. Failing to comply with requests from appropriate teachers or School District administrators to discontinue activities that threaten the operation or integrity of the CIS systems.

5. Content Regulations

Information electronically published on the School District's CIS system shall be subject to the following regulations:

a. Published documents, including but not limited to audio and video clips or conferences, may not include a student's date of birth, Social Security number, driver's license number, financial information, phone number(s), street address, or box number, name (other than first name), or the names of other family members without parental consent.

b. Documents, web pages, Electronic Communications, or videoconferences may not include personally identifiable information that indicates the physical location of a student at a given time without parental consent.

c. Documents, web pages, Electronic Communications, or videoconferences may not contain objectionable materials or point directly or indirectly to objectionable materials.

d. Documents, web pages, and Electronic Communications must conform to all School District Policies, regulations, rules, and procedures.

e. Documents to be published on the Internet must be edited and approved according to School District procedures before publication.

6. Due Process

   a. The School District will cooperate with the School District's ISP rules, local, state, and federal officials to the extent legally required in investigations concerning or relating to any illegal activities conducted through the School District's CIS systems.

   b. If students or employees possess due process rights for discipline resulting from the violation of this Policy, they will be provided such rights.

   c. The School District may terminate the account privileges by providing notice to the User.

7. Search and Seizure

   a. Users' violations of this Policy, any other School District Policies, regulations, rules, or procedures, ISP terms, or the law may be discovered by routine maintenance and monitoring of the School District's CIS system, or any method stated in this Policy, or pursuant to any legal means.

   b. The School District reserves the right, but not the duty, to inspect, review, or retain Electronic Communications created, sent, displayed, received, or stored on or over its CIS systems; to monitor, record, check, track, log, access, or otherwise inspect; and/or report all aspects of its CIS systems. This includes any personal Computers, network, Internet, Electronic Communications systems, databases, files, software, and media that they bring onto the School District's property, or to School District's events, that were connected to the School District network, and/or that contain School District programs, or School District or Users' data or information, all pursuant to law, in order to insure compliance with this Policy, other School District Policies, regulations, rules, and procedures, ISP terms, and local, state, and federal law in order to protect the School District's resources, and to comply with the law.

   c. Everything that Users place in their personal files should be written as if a third party will review it.

8. Copyright Infringement and Plagiarism

17 U.S.C. Sec. 1202
Pol. 814

   a. Federal laws, cases, Policies, regulations, and guidelines pertaining to copyright will govern the use of material accessed through the School District resources. See School District Copyright Policy. Users will make a standard practice of requesting permission from the holder of the work, and

complying with the Fair Use Doctrine, and/or complying with license agreements. Employees will instruct Users to respect copyrights, request permission when appropriate, and comply with the Fair Use Doctrine and/or with license agreements. Employees will respect and comply as well.

b. Violations of copyright law can be a felony, and the law allows a court to hold individuals personally responsible for infringing the law. The School District does not permit illegal acts pertaining to the copyright law. Therefore, any User violating the copyright law does so at his/her own risk and assumes all liability.

c. Violations of copyright law include but are not limited to making of unauthorized copies of any copyrighted material (such as commercial software, text, graphic images, audio and video recording), distributing copyrighted materials over Computer networks, remixing or preparing mash-ups, and deep-linking and framing into the content of others' websites. Further, the illegal installation of copyrighted software or files for use on the School District's Computers is expressly prohibited. This includes all forms of licensed software – shrink-wrap, clickwrap, browsewrap, and electronic software downloaded from the Internet.

d. No one may circumvent a Technology Protection Measure that controls access to a protected work unless they are permitted to do so by law. No one may manufacture, import, offer to the public, or otherwise traffic in any technology, product, service, device, component or part that is produced or marketed to circumvent a technology protection measure to control access to a copyright protected work.

e. School District guidelines on plagiarism will govern use of material accessed through the School District's CIS systems. Users must not plagiarize works that they find. Teachers will instruct students in appropriate research and citation practices. Users understand that use of the School District's CIS systems may involve the School District's use of plagiarism analysis software being applied to their works.

9. <u>Selection of Material</u>

a. School District Policies on the selection of materials will govern use of the School District's CIS systems.

b. When using the Internet for class activities, teachers must select material that is appropriate in light of the age of the students and that is relevant to the course objectives. Teachers must preview the materials and websites they

	require or recommend students access to determine the appropriateness of the material contained on or accessed through the website. Teachers must provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly. Teachers must assist their students in developing the critical thinking skills necessary to ascertain the truthfulness of information, distinguish fact from opinion, and engage in discussions about controversial issues while demonstrating tolerance and respect for those who hold divergent views.
17 U.S.C. Sec. 512	10. School District Website The School District has established a Website to present information about the School District and will maintain, modify, and develop its web pages under the direction of the Technology Manager and/or designee. Publishers must comply with this Policy, other Board Policies, School District regulations, rules, and procedures, for example the School District's Website Development Policy, ISP terms, and local, state, and federal laws. The School District may limit its liability by complying with the Digital Millennium Copyright Act's safe harbor notice and takedown provisions. 11. Blogging a. If an employee, student, or Guest creates a blog with his/her own resources, the employee, student, or Guest may not violate the privacy rights of employees and students; may not use School District personal and private information/data, images, and copyrighted material in his/her blog; and may not disrupt the School District. b. Conduct otherwise will result in actions further described in the Consequences for Inappropriate, Unauthorized and Illegal Use section of this Policy and provided in relevant School District Policies, regulations, rules, and procedures. 12. Safety and Privacy a. To the extent legally required, Users of the School District's CIS systems will be protected from harassment or commercially unsolicited Electronic Communications. Any User who receives threatening or unwelcome communications must immediately send or take them to the building principal and/or designee.

b. Users will not post personal contact information about themselves or other people on the CIS systems. Users may not steal another's identity in any way; may not use spyware, cookies, and other program code; and may not use School District or personal technology or resources in any way to invade one's privacy. Additionally, Users may not disclose, use, or disseminate confidential and personal information about students or employees. Examples include, but are not limited to, revealing biometric data, student grades, Social Security numbers, dates of birth, home addresses, telephone numbers, school addresses, work addresses, credit card numbers, health and financial information, evaluations, psychological reports, educational records, reports, and resumes or other information relevant to seeking employment at the School District, by using a PDA, iPhone, Blackberry, cell phone (with or without camera/video) and/or other Computer, unless authorized to do so by the building principal or immediate supervisor.

c. If the School District requires that data and information be encrypted, Users must use School District authorized encryption to protect their security.

d. Student users will agree not to meet with someone they have met online unless they have parental consent.

13. Consequences for Inappropriate, Unauthorized, and Illegal Use

a. General rules for behavior, ethics, and communications apply when using the CIS systems and information, in addition to the stipulations of this Policy, other School District Policies, regulations, rules, and procedures, ISP terms, and local, state, and federal laws. Users must be aware that violations of this Policy or other School District Policies, regulations, rules and procedures or for unlawful use of the CIS systems, may result in loss of CIS access and a variety of other disciplinary actions, including but not limited to, warnings, usage restrictions, loss of privileges, position reassignment, oral or written reprimands, student suspensions, employee suspensions (with or without pay), dismissals, expulsions, breach of contract, and/or legal proceedings on a case-by-case basis. This Policy incorporates all other relevant School District Policies, such as but not limited to, the student and professional employee discipline Policies, Code of Student Conduct, copyright, property, curriculum, terroristic threat, vendor access, and harassment Policies.

b. Users are responsible for damages to Computers, the network, equipment, Electronic Communications Systems, and software resulting from accidental, negligent, deliberate, and willful acts. Users will also be responsible for incidental or unintended damage resulting from negligent, willful, or deliberate violations of this Policy, other School District Policies,

regulations, rules, and procedures, ISP terms, and local, state, and federal laws. For example, Users will be responsible for payments related to lost or stolen Computers and/or School District equipment and recovery and/or breach of the data contained on them.

c. Violations as described in this Policy, other School District Policies, regulations, rules, and procedures may be reported to the School District and to appropriate legal authorities, whether the ISP, local, state, or federal law enforcement, and may constitute a crime under state and/or federal law, which may result in arrest, criminal prosecution, and/or lifetime inclusion on a sexual offenders registry. The School District will cooperate to the extent legally required with authorities in all such investigations.

d. Vandalism will result in cancellation of access to the School District's CIS systems and resources and will be subject to discipline.

e. Any and all costs incurred by the School District for repairs and/or replacement of software, hardware, and data files and for technological consultant services due to any violation of this Policy, other School District Policies, regulations, rules, and procedures, or ISP, local, state or federal law, must be paid by the User who caused the loss.

Original Adoption – February 10, 1997
Revised and Adopted – October 8, 2001
Revised and Adopted – October 8, 2007

References:

School Code – 24 P.S. Sec. 510, 1303.1-A

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

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, 830