

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF THE COMPUTERS, NETWORK, INTERNET, ELECTRONIC COMMUNICATIONS, AND INFORMATION POLICY

ADOPTED: January 24, 2002

REVISED: May 11, 2010  
November 8, 2011

# POTTSGROVE SCHOOL DISTRICT

<p>1. Purpose</p>	<p style="text-align: center;"><b>815.1. ACCEPTABLE USE OF THE COMPUTERS, NETWORK, INTERNET, ELECTRONIC COMMUNICATIONS, AND INFORMATION POLICY</b></p> <p>Pottsgrove School District (District) provides employees, students and guests (users) with access to the District’s electronic communication systems and network, which includes Internet access, whether wired or wireless, or by any other means.</p> <p>Computers, network, Internet, electronic communications and information systems (collectively CIS systems) provide vast, diverse and unique resources. The Board will provide access to the District’s CIS systems in order to access information, research, to facilitate learning and teaching, and to foster the educational purpose and mission of the District.</p> <p>For users, the District’s CIS systems must be used primarily for education-related purposes and performance of District job duties. 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. Personal use must comply with this policy and all other applicable District policies, procedures and rules contained in this policy, as well as Internet service provider (ISP) terms, local, state and federal laws and must not damage the District’s CIS systems. Students may only use the CIS systems for educational purposes. At the same time, employees’ and students’ personal technology devices brought onto the District’s property or suspected to contain District information may be legally accessed to ensure compliance with this policy and other District policies to protect the District’s resources, and to comply with the law.</p> <p>The District intends to strictly protect its CIS systems against numerous outside and internal risks and vulnerabilities. Users are important and critical players in protecting these District assets and in lessening the risks that can destroy these important and critical assets. Consequently, employees, students and guests are required to fully comply with this policy, and to immediately report any violations or suspicious activities to the Director of Technology and/or designee. Conduct otherwise will result in actions further described in Consequences For Inappropriate,</p>
-------------------	---

815.1. ACCEPTABLE USE OF THE COMPUTERS, NETWORK, INTERNET, ELECTRONIC COMMUNICATIONS, AND INFORMATION POLICY - Pg. 2

<p>2. Definitions</p>	<p>Unauthorized And Illegal Use, of this policy and provided in relevant District policies.</p> <ol style="list-style-type: none"><li>1. <b>Access to the Internet</b> - A computer shall be considered to have access to the Internet if the computer is equipped with a modem or is connected to a network that has access to the Internet, whether by wire, wireless, cable, or any other means.</li><li>2. <b>Child Pornography</b> - 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:<ol style="list-style-type: none"><li>a. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct.</li><li>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 is not engaged in sexually explicit conduct but is created, stored, downloaded/uploaded or enhanced and is used or stored for the sole purpose of sexual self gratification of the viewer/creator.</li><li>c. Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.</li></ol></li><li>3. <b>Computer</b> - Includes any District owned, leased or licensed or employee, student and guest owned personal hardware, software, or other technology used on District premises or at District events, or connected to the District network, containing District programs or 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, District, employee, students and guest: desktop, notebook, powerbook, tablet PC or laptop computers, printers, cables, modems, and other peripherals; specialized electronic equipment used for student's special educational purposes; global position system (GPS) equipment; personal digital assistants (PDAs); cell phones, with or without Internet access and/or recording and/or camera and other capabilities, mobile phones, or wireless devices; beepers; paging devices, laser pointers and attachments, and any other such technology developed.</li></ol>
-----------------------	--

815.1. ACCEPTABLE USE OF THE COMPUTERS, NETWORK, INTERNET, ELECTRONIC COMMUNICATIONS, AND INFORMATION POLICY - Pg. 3

4. **Electronic Communications System** - Any messaging, collaboration, publishing, broadcast, telephone 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, photo optical or photo electronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications. Examples include, but are not limited to, the Internet, intranet, electronic mail services, Global Positioning Systems, Personal Digital Assistants, facsimile machines, cell phones with or without Internet access and/or electronic mail and/or recording devices, cameras, and other capabilities.
5. **Educational Purpose** - Includes use of the CIS systems for classroom activities, professional development, and to support the District's curriculum, policy and mission statement.
6. **Harmful To Minors** - 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.
  - c. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.
7. **Incidental Personal Use** - Use of District CIS systems by an individual employee for occasional personal communications. Personal use must comply with this policy and all other District policies, procedures and rules, as well as ISP, local, state and federal laws and may not interfere with the employee's job duties and performance, with system operations, storage capacity, intranet/extranet/LAN/WAN bandwidth, or with other system users, and must not damage the District's CIS systems. Under no circumstances should the employee believe their use is private. The District reserves the right to monitor, track, access, and log the use of its CIS systems at any time.

815.1. ACCEPTABLE USE OF THE COMPUTERS, NETWORK, INTERNET, ELECTRONIC COMMUNICATIONS, AND INFORMATION POLICY - Pg. 4

<p>3. Authority</p>	<p>8. <b>Minor</b> - For purposes of compliance with the Children’s Internet Protection Act (CIPA), an individual who has not yet attained the age of seventeen (17). For other purposes, <b>minor</b> shall mean the age of minority as defined in the relevant law.</p> <p>9. <b>Network</b> - A system that links two (2) or more computer systems, including all components necessary to effect the operation, including, but not limited to: computers, copper and fiber cabling, wireless communications and links, equipment closets and enclosures, network electronics, telephone lines, printers and other peripherals, storage media, software, and other computers and/or networks to which the network may be connected, such as the Internet or those of other institutions.</p> <p>10. <b>Obscene</b> - Analysis of the material meets the following elements:</p> <ul style="list-style-type: none"><li>a. Whether the average person, applying contemporary community standards, would find that the material, taken as a whole, appeals to the prurient interest.</li><li>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.</li><li>c. Whether the work taken as a whole lacks serious literary, artistic, political, or scientific value.</li></ul> <p>11. <b>Sexual Act And Sexual Contact</b> - As defined at 18 U.S.C. § 2246(2), and at 18 U.S.C. § 2246(3), 18 Pa. C.S.A. § 5903.</p> <p>12. <b>Technology Protection Measure(s)</b> - A specific technology that blocks or filters Internet access to and e-mail containing visual depictions that are obscene, child pornography or harmful to minors.</p> <p>13. <b>Visual Depictions</b> - Undeveloped film and videotape and data stored on computer disk or by electronic means which is capable of conversion into a visual image but does not include only words.</p> <p>Access to the District's CIS systems through school resources is a privilege, not a right. These, as well as the user accounts and information, are the property of the District, which reserves the right to deny access to prevent further unauthorized, inappropriate or illegal activity, and may revoke those privileges and/or administer appropriate disciplinary action. The District will cooperate to the extent legally</p>
---------------------	---

815.1. ACCEPTABLE USE OF THE COMPUTERS, NETWORK, INTERNET, ELECTRONIC COMMUNICATIONS, AND INFORMATION POLICY - Pg. 5

<p>20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254</p>	<p>required with the ISP, local, state and federal officials in any investigation concerning or related to the misuse of the CIS systems.</p> <p>It is often necessary to access user accounts in order to perform routine maintenance and security tasks; system administrators have the right to access by interception, and the stored communication of user accounts for any reason in order to uphold this policy and to maintain the system. Users have no privacy expectation in the contents of their personal files or any of their use of the District's CIS systems. The District reserves the right to monitor, track, log and access CIS systems use and to monitor and allocate client computer (PC) and files server space.</p> <p>The District reserves the right to restrict access to any Internet sites or functions it may deem inappropriate through software blocking or general policy. Specifically, the District operates and enforces technology protection measure(s) that block or filter e-mail and online activities of minors on its computers used and accessible to adults and students so as to filter or block inappropriate matter on the Internet and via e-mail. Inappropriate matter includes, but is not limited to, visual, graphic, text and any other form of obscene, sexually explicit, child pornographic, or other material that is harmful to minors, hateful, illegal, defamatory, lewd, vulgar, profane, rude, 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, terroristic, and advocates the destruction of property.</p> <p>The District has the right, but not the duty, to monitor, track, log, access and report all aspects of its computer information technology and related systems of all users and of any employee's, student's and guest's personal computers, network, Internet, electronic communication systems, and media brought on to District premises or at District events, connected to the District premises or at District events, connected to the District network, containing District programs or District or student data (including images, files, and other information) to ensure compliance with this policy and other District policies, to protect the District's resources, and to comply with the law.</p> <p>The District reserves the right to restrict or limit usage of lower priority CIS systems and computer uses when network and computing requirements impact available capacity according to the following priorities:</p> <ol style="list-style-type: none"><li>1. Highest - uses that directly supports the education of students.</li><li>2. Medium - uses that indirectly benefit the education of the student.</li></ol>
---	--

815.1. ACCEPTABLE USE OF THE COMPUTERS, NETWORK, INTERNET, ELECTRONIC COMMUNICATIONS, AND INFORMATION POLICY - Pg. 6

3. Lowest - uses that include reasonable and limited educationally-related interpersonal communications and incidental personal communications.

4. Forbidden - all activities in violation of this policy.

The District additionally reserves the right to:

1. Determine which CIS systems services will be provided through District resources.
2. View and monitor network traffic, file server and client computer (PC) disk space, processor, RAM and system utilization, and all applications provided through the network and communications systems, including e-mail.
3. Remove excess e-mail or files taking up an inordinate amount of client computer (PC) and fileserver disk space after a reasonable time or if they are interfering with normal system function.
4. Revoke user privileges, remove user accounts, or refer to legal authorities when violation of this and any other applicable District policies occur or state or federal law is violated, including, but not limited to, those governing network use, copyright, security, privacy, employment, and destruction of District resources and equipment.

Responsibility

1. Due to the nature of the Internet as a global network connecting thousands of computers around the world, inappropriate materials, including those which may be defamatory, discriminatory (as it pertains to race, color, religion, national origin, gender, marital status, age, sexual orientation, political beliefs, receipt of financial aid, or disability), inaccurate, obscene, sexually explicit, lewd, vulgar, rude, harassing, violent, inflammatory, threatening, terroristic, hateful, bullying, profane, pornographic, offensive, and illegal, can be accessed through the network and electronic communications systems. Because of the nature of the technology that allows the Internet to operate, the District cannot completely block access to these resources. Accessing these and similar types of resources shall be considered an unacceptable use of school resources and will result in actions explained further in Consequences For Inappropriate, Unauthorized And Illegal Use, of this policy and as provided in relevant District policies.
2. Employees must become proficient in the use of the District's CIS systems, and software relevant to the employee's responsibilities and practice proper netiquette, District ethics, and agree to the requirements of this policy.

815.1. ACCEPTABLE USE OF THE COMPUTERS, NETWORK, INTERNET, ELECTRONIC COMMUNICATIONS, AND INFORMATION POLICY - Pg. 7

<p>4. Delegation of Responsibility</p>	<p>The Director of Technology and/or designee will serve as the coordinator to oversee the District's CIS systems and will work with other regional or state organizations as necessary, to educate employees, 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 ensure adequate supervision of the CIS systems, maintain executed user agreements, and interpret and enforce this policy.</p> <p>The Director of Technology and/or designee will establish a process for setting-up individual and class accounts, set quotas for disk usage on the system, establish a retention schedule, and establish the District virus protection process. 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 District and District CIS systems, and to abide by the rules established by the District, its ISP(s), local, state and federal laws.</p>
<p>5. Guidelines</p>	<p><u>Access To The CIS Systems</u></p> <p>CIS systems user accounts will be used only by authorized owners of the accounts for authorized purposes.</p> <p>An account will be made available according to a procedure developed by appropriate District authorities.</p> <p><u>CIS System</u></p> <p>The District's Acceptable Use of the Computers, Network, Internet, Electronic Communications, and Information Policy, as well as other relevant District policies, will govern use of the District's CIS systems for students, employees and guests. Use of the CIS systems will also be governed by the other relevant District policies.</p> <p>Types of services included, but not limited to:</p> <ol style="list-style-type: none"> <li>1. Network Services - District employees, students, and guests will have access to District Network Services. The Director of Technology or designee will establish procedures and guidelines for authentication (password security and syntax) that will consist of no less than six letters and number for general network access and no less than eight letters, numbers and special symbols to access the District's student information system (SIS). SIS passwords will be set to expire no fewer than every thirty school days but not to exceed ninety days.</li> </ol>

815.1. ACCEPTABLE USE OF THE COMPUTERS, NETWORK, INTERNET, ELECTRONIC COMMUNICATIONS, AND INFORMATION POLICY - Pg. 8

2. Internet - District employees, students, and guests will have access to the Internet through the District's CIS systems as needed.
3. E-Mail - District employees may be provided assigned individual e-mail accounts for work related, and incidental personal use, as needed. Students may be assigned individual e-mail accounts, as necessary, by the Network Services Manager or designee. Teachers will supervise the students' use of the e-mail service.
4. Personally Identifiable Information - You may send e-mail messages to individual students, groups of students, parents/guardians, and to other employees who possess an educational interest in the student(s) at issue in the e-mail. Messages sent to a group of students, must be for school purposes only and shall not contain any confidential or protected information about an individual student.

The District uses e-mail messages for official communication therefore; all users are required to read and/or respond to messages containing official business within a reasonable time frame. Users are required to follow established mailbox maintenance guidelines established by the Director of Technology and/or designee. Users are responsible for the consequences of not checking their e-mail or performing mailbox maintenance on a regular basis. The District will not be responsible for e-mail messages that are lost, misrouted, delayed, or misdirected. The District has the right, but not the duty to monitor all employees e-mail messages. Even though general e-mail is an official form of school business, it is not a secure means of communication to transmit sensitive or protected data. Below are some guidelines.

Privacy And Security

1. FERPA gives parents/guardians and eligible students the right to request that certain information not be made public. Therefore, some may elect to not have student contact information (such as, e-mail addresses) published in District public directories or communicated beyond the District's network or e-mail system or course setting.
2. No specific personal or personally identifiable information shall be released to any individual over the telephone, by e-mail or voice mail message. Directory information may be released, if it does not invade the privacy of the student, however, if the parent/guardian has indicated on the annual Directory Information Notice that no information may be released for their child no such information may be disclosed. Directory information may include the student's name, degrees and awards received, participation in officially recognized

815.1. ACCEPTABLE USE OF THE COMPUTERS, NETWORK, INTERNET, ELECTRONIC COMMUNICATIONS, AND INFORMATION POLICY - Pg. 9

<p>Pol. 216</p>	<p>activities or sports. Other uses of e-mail includes obtaining homework and instructional material, explaining work and homework, asking for information and references, obtaining lost handouts or assignment sheets and explaining absences.</p> <ol style="list-style-type: none"><li>3. Other people can read your e-mail while it is in transit, and the recipient can transfer the e-mail message to those s/he chooses.</li><li>4. E-mail, chat rooms, electronic bulletin boards, text messaging and other electronic communications are not appropriate for transmitting sensitive or confidential information. Confidentiality for such messages is protected by FERPA, and other privacy laws such as HIPAA and PPRA.</li><li>5. All use of e-mail must be consistent with the District’s Student Record’s Policy and Plan. Remember that the recipient has the right to redirect (forward) or share your message with others. You are responsible for ensuring that the message is accurately sent and the message is sent at your own risk.</li><li>6. You must include in the e-mail subject line and leading lines of the body of the e-mail text “CONFIDENTIAL – (___Insert Student’s Name___). DO NOT DISCLOSE OR REDISCLOSE).” See attached Parent/Guardian Consent for a Student’s Personally Identifiable Information to be sent by electronic mail form.</li><li>7. When you find that it is necessary to provide information in an e-mail that has personally identifiable information, you should speak in general terms, i.e., explain policies and/or procedures for situations without confirming or denying personal information.</li></ol> <p><u>Use</u></p> <ol style="list-style-type: none"><li>1. The District will not be responsible for your infrequent and inconsistent access of your e-mail messages to stay current with District communications.</li><li>2. You are required to explain to students how e-mail will be used in your class, and provide the students with the e-mail requirements and expectations. For example, will you be responding to e-mail messages from parents/guardians and/or students on weekends, evenings, holidays, or when you are away? Does the District have a policy pertinent to this requirement for you to follow? Will you use your out-of-office e-mail response to messages?</li><li>3. E-mail messages are to be used to provide academic and administrative support to the students in order to enhance their educational experience.</li></ol>
-----------------	--

815.1. ACCEPTABLE USE OF THE COMPUTERS, NETWORK, INTERNET, ELECTRONIC COMMUNICATIONS, AND INFORMATION POLICY - Pg. 10

4. You are expected to report any actual or suspected breaches of confidential information to the Assistant Superintendent.
5. Consent may be obtained from a parent/guardian in an e-mail message if the employee has reasonable belief that the e-mail address is credible.
6. You must be certain that the information you transmit is factually accurate and carefully identified as a personal opinion so as to avoid a claim of defamation. You are expressly required not to make any defamatory statements and not to infringe or authorize any infringement of copyright or any other legal right by e-mail communications. Any communication of this nature is contrary to District policy and outside the scope of your employment. The District will not accept any liability in respect of such communication, and you will be personally liable for any damages or other liability arising.
7. You are not authorized to conclude any binding agreement on behalf of the District with another party by e-mail.
8. E-mails are documents that can be used in legal proceedings. They should be carefully written and sent only to the appropriate recipients.
9. Disclaimer: Users are not permitted to create their own e-mail disclaimer. The following disclaimer will be added to all outbound e-mails at the system level: "This e-mail and any files transmitted with it are to be treated as confidential and as such are not be used or disclosed except for the purpose for which it has been sent. Any views or opinions presented in this e-mail are solely those of the author and do not represent those of the Pottsgrove School District. The District accepts no liability for any damage caused by this e-mail. The recipient is required to indemnify the District against any claims for loss or damage caused by any viruses or otherwise."

The District will not be responsible for your violation of a student's privacy due to your e-mail use, and the District will discipline you as provided in the District's contracts, policies and practices.

Guest Accounts

Guests, which include but are not limited to, independent contractors and adult education instructors, may receive an individual account with the approval of the Director of Technology and/or designee if there is a specific, District-related purpose requiring such access. Use of the CIS systems by a guest must be specifically limited to the District-related purpose. A signed written agreement will be required and parental signature will be required if the guest is a minor.

815.1. ACCEPTABLE USE OF THE COMPUTERS, NETWORK, INTERNET, ELECTRONIC COMMUNICATIONS, AND INFORMATION POLICY - Pg. 11

An open guest network with filtered access to the Internet but no other CIS network services can be maintained at the discretion of the Director of Technology and/or designee. Persons accessing the Internet through the open guest network do so at their own risk. The District assumes no responsibility for mishaps to the guest's device resulting from connectivity. Guests using the open network agree to all applicable provision of this policy and other applicable District policies.

Access to all data on, taken from, or compiled using District computers is subject to inspection and discipline. Users have no right to expect that District information placed on users' personal computers, networks, Internet, and electronic communications systems is beyond the access of the District. The District reserves the right to legally access users' personal equipment for District information.

Parental Notification And Responsibility

The District will notify the parents/guardians about the District CIS systems and the policies governing their use. This policy contains restrictions on accessing inappropriate material. 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 not practically possible for the District to monitor and enforce a wide range of social values in student use of the Internet. Further, the District recognizes that parents/guardians bear primary responsibility for transmitting this particular set of family values to their children. The District will encourage parents/guardians to specify to their child(ren) what material is and is not acceptable for their child(ren) to access through the District's CIS system.

District Limitation Of Liability

The District makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the District's CIS systems will be error free or without defect. The District does not warrant the effectiveness of Internet filtering. The electronic information available to users does not imply endorsement of the content by the District, nor is the District responsible for the accuracy or quality of the information obtained through or stored on the CIS systems. The District shall 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 computers, network and electronic communications systems. The District shall not be responsible for material that is retrieved through the Internet, or the consequences that may result from them. The District shall not be responsible for any unauthorized financial obligations, charges or fees resulting from access to the District's CIS systems. In no event shall the District be liable to the user for any damages whether direct, indirect, special or consequential, arising out the use of the CIS systems.

815.1. ACCEPTABLE USE OF THE COMPUTERS, NETWORK, INTERNET, ELECTRONIC COMMUNICATIONS, AND INFORMATION POLICY - Pg. 12

Prohibitions

The use of the 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 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 are in effect any time District resources are accessed whether on District property, when using mobile commuting equipment, telecommunication facilities in unprotected areas or environments, directly from home, or indirectly through another ISP, and if relevant, when an employee, student or guest uses their own equipment.

General Prohibitions

Users are prohibited from using District CIS systems to:

1. Communicate about nonwork or nonschool-related communications unless the employees' use comports with this policy's definition of incidental personal use.
2. Access or transmit material that is harmful to minors, indecent, obscene, pornographic, child pornographic, terroristic, or advocates the destruction of property.
3. Access or transmit material likely to be offensive or objectionable to recipients including, but not limited to, that which may be defamatory, inaccurate, obscene, sexually explicit, lewd, hateful, 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, vulgar, rude, inflammatory, threatening, profane, pornographic, offensive, terroristic and/or illegal.
4. Cyber bullying another individual.
5. Access or transmit gambling, pools for money, including but not limited to: basketball and football, or any other betting or games of chance.
6. 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.

815.1. ACCEPTABLE USE OF THE COMPUTERS, NETWORK, INTERNET, ELECTRONIC COMMUNICATIONS, AND INFORMATION POLICY - Pg. 13

<p>Pol. 814</p>	<ol style="list-style-type: none"><li>7. Send terroristic threats, hateful e-mail, harassing communications, discriminatory remarks, and offensive or inflammatory communications.</li><li>8. Participate in unauthorized Internet Relay Chats, gaming, 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.</li><li>9. Facilitate any illegal activity.</li><li>10. Communicate through e-mail for non-educational purposes or activities, unless it is for an incidental personal use as defined in this policy. 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).</li><li>11. Engage in commercial, for-profit, or any business purposes (except where such activities are otherwise permitted or authorized under applicable District policies); conduct unauthorized fundraising or advertising on behalf of the District and nonschool District organizations; resell of District computer resources to individuals or organizations; or use the District's name in any unauthorized manner that would reflect negatively on the District, its employees, or students. Commercial purposes is defined as offering or providing goods or services or purchasing goods or services for personal use. District acquisition policies will be followed for District purchase of goods or supplies through the District system.</li><li>12. Political lobbying.</li><li>13. Install, distribute, reproduce or use any software (copyrighted or not), plug-ins, downloaded executables, batch file or batch processes, or operating system updates on District computers, or copy District software to unauthorized computer systems, intentionally infringing upon the intellectual property rights of others or violating a copyright. See the Copyright Infringement section of this policy and the District's Copyright Policy for additional information. All software must be reviewed and approved by the Director of Technology and/or designee, for system compliance, prior to purchase or installation.</li></ol>
-----------------	--

815.1. ACCEPTABLE USE OF THE COMPUTERS, NETWORK, INTERNET, ELECTRONIC COMMUNICATIONS, AND INFORMATION POLICY - Pg. 14

14. Encrypt messages using encryption software that is not authorized by the District from any access point on District equipment or District property. Employees, students and guests must use District approved encryption to protect the confidentiality of sensitive or critical information in the District's approved manner.
15. Access, interfere, possess, or distribute confidential or private information including messages sent privately, without permission of the person who sent the message.
16. Violate the privacy or security of electronic information.
17. Use the systems to send any District information to another party, except in the ordinary course of business as necessary or appropriate for the advancement of the District's business, or educational interest.
18. Sending unsolicited commercial electronic mail messages, also known as spam.

Access And Security Prohibitions

Users must immediately notify the Director of Technology and/or designee if they have identified a possible security problem. Students, employees, and guests must read, understand and comply with this policy that includes network, Internet usage, electronic communications, telecommunications, non-disclosure and physical information security policies. The following activities related to access to the District's CIS systems, and information are prohibited:

1. Misrepresentation (including forgery) of the identity of a sender or source of communication.
2. Acquiring or attempting to acquire passwords of others or giving your password to another. Users will be held responsible for the result of any misuse of the users' user name or password while the users' systems access were left unattended and accessible to others, whether intentional or through negligence.
3. Using or attempting to use computer accounts of others, these actions are illegal, even with consent, or if only for the purpose of "browsing".
4. Altering a communication originally received from another person or computer with the intent to deceive.

815.1. ACCEPTABLE USE OF THE COMPUTERS, NETWORK, INTERNET, ELECTRONIC COMMUNICATIONS, AND INFORMATION POLICY - Pg. 15

5. Using 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 of any kind, or being involved in a terroristic threat against any person or property, including cyber bullying.
6. Disabling or circumventing any District security, program or device, for example, but not limited to, anti-spyware, anti-spam software, and virus protection software or procedures.
7. Transmitting electronic communications anonymously or under an alias unless authorized by the District.

Operational Prohibitions

The following operational activities and behaviors are prohibited:

1. Interference with 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 and trapdoor program code, the sending of electronic chain mail, distasteful jokes, and the inappropriate sending of “broadcast” messages to large numbers of individuals or hosts. The user may not hack or crack the network (unless authorized by the Director of Technology and/or designee for security testing) or others’ computers, whether by parasiteware or 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 (unless authorized by the Director of Technology and/or designee for testing, help services or repair) a person’s computer, or to “look around”.
2. Altering or attempting to alter files, system security software or the systems without authorization.
3. Unauthorized scanning of the CIS systems for security vulnerabilities unless authorized.
4. Attempting to alter any District computing or networking components (including, but not limited to file servers, bridges, routers, or switches) without authorization or beyond one’s level of authorization.

815.1. ACCEPTABLE USE OF THE COMPUTERS, NETWORK, INTERNET, ELECTRONIC COMMUNICATIONS, AND INFORMATION POLICY - Pg. 16

5. 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, or by other means.
6. Connecting unauthorized hardware and devices to the CIS systems.
7. Loading, downloading, or use of unauthorized games, programs, files, or other electronic media, including, but is not limited to, downloading music files.
8. Intentionally damaging or destroying the integrity of the District's electronic information.
9. Intentionally destroying the District's computer hardware or software.
10. Intentionally disrupting the use of the CIS systems.
11. Damaging the District's CIS systems or networking equipment through the users' negligence or deliberate act.
12. Failing to comply with requests from appropriate teachers, District administrators or the Director of Technology and/or designee to discontinue activities that threaten the operation or integrity of the CIS systems.

Content Guidelines

Information electronically published on the District's CIS systems shall be subject to the following guidelines:

1. Published documents including but not limited to audio and video clips or conferences, may not include a child's phone number, street address, or box number, name (other than first name) or the names of other family members without parental consent.
2. 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.
3. Documents, web pages, electronic communications, or videoconferences may not contain objectionable materials or point directly or indirectly to objectionable materials.

815.1. ACCEPTABLE USE OF THE COMPUTERS, NETWORK, INTERNET, ELECTRONIC COMMUNICATIONS, AND INFORMATION POLICY - Pg. 17

4. Documents, web pages and electronic communications, must conform to all District policies and guidelines, including the copyright policy.
5. Documents to be published on the Internet must be edited and approved according to District procedures before publication.

Due Process

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

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

The District may terminate the account privileges by providing notice to the user.

Search And Seizure

User's violations of this policy, any other District policy, or the law may be discovered by routine maintenance and monitoring of the District system, or any method stated in this policy, or pursuant to any legal means.

The District reserves the right to monitor, track, log and access any electronic communications, including but not limited to, Internet access and e-mails at any time for any reason. Users should not have the expectation of privacy in their use of the District CIS systems, and other District technology, even when used for personal reasons. Further, the District reserves the right, but not the obligation, to access any personal technology device of users brought onto the District's premises or at District events, or connected to the District network, containing District programs or District or student data (including images, files, and other information) to ensure compliance with this policy and other District policies, to protect the District's resources, and to comply with the law.

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

Copyright Infringement And Plagiarism

Federal laws, cases, and guidelines pertaining to copyright will govern the use of material accessed through the District resources. Users will make a standard practice of requesting permission from the holder of the work and complying with license

Pol. 814

815.1. ACCEPTABLE USE OF THE COMPUTERS, NETWORK, INTERNET, ELECTRONIC COMMUNICATIONS, AND INFORMATION POLICY - Pg. 18

agreements. Employees will instruct students to respect copyrights, request permission when appropriate, and comply with license agreements and employees will respect and comply as well.

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

Violations of copyright law include, but are not limited to, the 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, and deep-linking and framing into the content of others' web sites. Further, the illegal installation of copyrighted software or files for use on the District's computers is expressly prohibited. This includes all forms of licensed software – shrink wrap, click wrap, browse wrap, and electronic software downloaded from the Internet.

District guidelines on plagiarism will govern use of material accessed through the District's CIS systems. Users will not plagiarize works that they find. Teachers will instruct students in appropriate research and citation practices.

Selection Of Material

Board policies on the selection of materials will govern use of the District's CIS systems.

When using the Internet for class activities, teachers will select material that is appropriate to the age of the students and that is relevant to the course objectives. Teachers will preview the materials and web sites they require or recommend students access to determine the appropriateness of the material contained on or accessed through the web site. Teachers will provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly. Teachers will 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. Any web site currently blocked by the District filtering software will not be opened/unblocked for review until the Director of Technology and/or designee has had the opportunity to review the site to determine why it is being blocked. Teachers are to request this review via the technology work request system.

815.1. ACCEPTABLE USE OF THE COMPUTERS, NETWORK, INTERNET, ELECTRONIC COMMUNICATIONS, AND INFORMATION POLICY - Pg. 19

District Web Site

The District will establish and maintain a Web Site and will develop and modify its web pages that will present information about the District under the direction of the Director of Technology. Publishers must comply with the District's acceptable use guidelines.

Safety And Privacy

To the extent legally required, users of the District's CIS systems will be protected from harassment or commercially unsolicited electronic communication. Any user who receives threatening or unwelcome communications must immediately take them to the Chief Technology Officer and/or designee.

Users will not post personal contact information about themselves or other people on the CIS systems. The user may not steal another's identity in any way, may not use spyware, parasiteware, cookies, or use District or personnel employee technology or resources in any way to invade one's privacy. Additionally, the user may not disclose, use or disseminate confidential and personal information about students or employees (examples include, but are not limited to, using a cell phone with camera and Internet access to take pictures of anything, including but not limited to, persons, places, and documents relevant to the District, saving, storing and sending the image with or without text or disclosing them by any means, including but not limited to, print and electronic matter; revealing student grades, social security numbers, 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 District unless legitimately authorized to do so).

Consequences For Inappropriate, Unauthorized And Illegal Use

General rules for behavior, ethics, and communications apply when using the CIS systems and information, in addition to the stipulations of this policy. Users must be aware that violations of this policy or other policies, or for unlawful use of the CIS systems will 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, suspensions (with or without pay for employees), dismissal, expulsions, and/or legal proceedings on a case-by-case basis. This policy incorporates all other relevant District policies, such as, but not limited to, the student and professional employee discipline policies, copyright policy, property policy, curriculum policies, terroristic threat policy, and harassment policies.

815.1. ACCEPTABLE USE OF THE COMPUTERS, NETWORK, INTERNET, ELECTRONIC COMMUNICATIONS, AND INFORMATION POLICY - Pg. 20

The user is responsible for damages to the network, equipment, electronic communications systems, and software resulting from deliberate and willful acts. The user will also be responsible for incidental or unintended damage resulting from willful or deliberate violations of this policy.

Violations as described in this policy will be reported to the District and may be reported to the appropriate legal authorities, whether the ISP, local, state, or federal law enforcement. The District will cooperate to the extent legally required with authorities in all such investigations.

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

I have read and understand this policy and will comply with it. Additionally, I understand that if I violate the policy, I am subject to the District's discipline and could be subject to ISP, as well as local, state and federal legal recourse.

\_\_\_\_\_

Date

\_\_\_\_\_

Student or Employee's Name

Or

\_\_\_\_\_

Date

\_\_\_\_\_

Vendor Name

References:

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

Enhancing Education Through Technology Act of 2001 – 20 U.S.C. Sec. 6777

Internet Safety – 47 U.S.C. Sec. 254

Board Policy – 216, 814