



Section: Operations

Title: Acceptable Use of the Computers, Network, Internet, Electronic Communications and Information Systems Policy

Adopted: April 21, 2005

Revised: August 19, 2010

815. Acceptable Use of the Computers, Network, Internet, Electronic Communications and Information Systems Policy

Purpose The Colonial School District (“School District”) provides employees, students, school board members, and guests (“users”) with access to the School District’s electronic communication systems and network, which includes Internet access, whether wired or wireless, or by any other means.

Computers, network, Internet, electronic communications and information systems (collectively “CIS systems”) provide vast, diverse and unique resources. The Board will provide access to the School District’s CIS systems for users in order to access information, research, and collaborate to facilitate learning and teach to foster the educational purpose and mission of the School District.

For users, the School District’s CIS systems must be used primarily for education-related purposes and performance of School 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 School 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 School 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 School District’s property or suspected to contain School District information may be legally accessed to insure compliance with this Policy and other School District Policies to protect the School District’s resources, and to comply with the law. Users may not use their personal computers to access the School District’s intranet, Internet or any other CIS System unless approved by the Chief Information Officer and/or designee.

The School 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 School District assets and in lessening the risks that can destroy these important and critical assets. Consequently, users are required to fully comply with this policy, and to immediately report any violations or suspicious activities to the Building Administrator and/or District Chief Information Officer. Conduct otherwise will result in actions further described in Section 12 - Consequences for Inappropriate, Unauthorized and Illegal Use, found in the last Section of this Policy, and provided in relevant School District policies.

The District Faculty and Administration shall, to the extent practical, take steps to promote the safety and security of users of the District's online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.

It shall be the responsibility of all members of the District Faculty, Staff and Administration to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, Policy 221 (relating to bullying prevention), the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

Definitions

1. Access to the Internet – 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.

2. 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.

Under Pennsylvania law, any book, magazine, pamphlet, slide, photograph, film,

videotape, computer depiction or other material depicting a child under the age of 18 years engaging in a prohibited sexual act or in the simulation of such act.

3. Computer – Includes any School District owned, leased or licensed or user owned personal hardware, software, or other technology 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, School District and users: desktop, notebook, powerbook, tablet PC or laptop computers, printers, cables, modems, and other peripherals; specialized electronic equipment used for students' 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/video and other capabilities, mobile phones, or wireless devices, two-way radios/telephones; beepers; paging devices, laser pointers and attachments, and any other such technology developed.
4. 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 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/video, and other capabilities.
5. Educational Purpose - Includes use of the CIS systems for classroom activities, professional or career development, and to support the School District's curriculum, policy and mission statement.
6. 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.

Under Pennsylvania law, 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.

- 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. Personal use must comply with this policy and all other applicable School 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 School District's CIS systems.
- 8. Minor – For purposes of compliance with the Children's Internet Protection Act ("CIPA"), an individual who has not yet attained the age of seventeen. For other purposes, minor shall mean the age of minority as defined in the relevant law.
- 9. Network – A system that links two 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.

10. 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.

Under Pennsylvania law, analysis of the material meets the following elements:

- a. the average person, applying contemporary community standards, would find that the 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.
11. Sexual Act and Sexual Contact – As defined at 18 U.S.C. § 2246(2), and at 18 U.S.C. § 2246(3), 18 Pa.C.S.A. § 5903.
 12. 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.
 13. Visual Depictions – 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 mere words.

Authority

1. Access to the School 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 School 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 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 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 School District's CIS systems. The School District reserves the right to monitor, track, log and access CIS systems use and to monitor and allocate fileserver space.
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 on the Internet. 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. Measures designed to restrict adults' and minors' access to material harmful to minors may be disabled to enable an adult or student 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. Expedited review and resolution of a claim that the policy is denying a student or adult to access material will be enforced by an administrator, supervisor, or their designee upon the receipt of a written consent from a parent or guardian for a student, and upon the written request from an employee.
4. The School 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 user's personal computers, network, Internet, electronic communication systems, and media brought on to School District premises or at School District events, connected to the School District network, containing School District

programs or School District or student data (including images, files, and other information), pursuant to the law, to insure compliance with this policy and other School District policies, to protect the School District's resources, and to comply with the law.

5. 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 supports the education of the students.
 - b. Medium – uses that indirectly benefit the education of the student.
 - c. Lowest – uses that include reasonable and limited educationally-related interpersonal communications and incidental personnel communications.
 - d. Forbidden – all activities in violation of this policy.
6. The School District additionally reserves the right to:
 - a. Determine which CIS systems services will be provided through School District resources.
 - b. View and monitor network traffic, file server space, processor, and system utilization, and all applications provided through the network and communications systems, including e-mail.
 - c. Remove excess e-mail or files taking up an inordinate amount of file server disk space after a reasonable time.
 - d. Revoke user privileges, remove user accounts, or refer to legal authorities when violation of this and any other applicable School 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 School 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 School District cannot completely block access to these resources. Accessing these and similar types of resources may be considered an unacceptable use of school resources and will result in actions explained further in Section 12 Consequences for Inappropriate, Unauthorized and Illegal Use, found in the last Section of this policy and as provided in relevant School District policies.

2. Employees must be capable and able to use the School District's CIS systems, and software relevant to the employee's responsibilities. In addition, Users must practice proper etiquette, School District ethics, and agree to the requirements of this policy.
 - a. Etiquette users are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to the following:
 - (1) Be polite. Do not become abrasive in messages to others. General School District rules and policies for behavior and communicating apply.
 - (2) Use appropriate language. Do not swear or use vulgarities or other inappropriate language.
 - (3) Do not reveal the personal addresses or telephone numbers of others.
 - (4) Recognize that e-mail is not private or confidential.
 - (5) Do not use the Internet or e-mail in any way that would interfere with or disrupt its use by other users.
 - (6) Consider all communications and information accessible via the Internet to be the property of the School District.
 - (7) Do not order any materials or use credit cards while using the School District's computers except for educational or work related purposes.
 - (8) Respect the rights of other users to an open and hospitable technology environment, regardless of race,

sexual orientation, color, religion, creed, ethnicity, age, marital status or handicap status.

Delegation of Responsibility

1. The Chief Information Officer 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 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 insure adequate supervision of the CIS systems, maintain executed user agreements, and interpret and enforce this policy.
2. The Chief Information Officer 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 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 rules established by the School District, its ISP, local, state and federal laws.

Guidelines

1. Access to the CIS Systems
 - a. CIS systems user accounts will be used only by authorized owners of the accounts for authorized purposes.
 - b. An account will be made available according to a procedure developed by appropriate School District authorities.
 - c. CIS System. The School District's Acceptable Use of the Computers, Network, Internet, Electronic Communications and Information Systems Policy, as well as other relevant School District policies, will govern use of the School District's CIS systems for users. Users' use of the CIS systems will also be governed by the other relevant School District policies.
 - d. Types of Services included, but not limited to:

- (1) World Wide Web. School District employees and students will have access to the Web through the School District's CIS systems as needed.
 - (2) E-Mail. School District employees may be provided assigned individual e-mail accounts for work related use, as needed. Students may be assigned individual e-mail accounts, as necessary, by the Director of Technology and/or designee at the recommendation of the teacher who will also supervise the students' use of the e-mail service.
 - (3) Guest Accounts. Guests, which includes but are not limited to, visitors, workshop attendees, volunteers, independent contractors, and adult education teachers and students, may receive an individual account with the approval of the Chief Information Officer 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. An agreement will be required and parental signature will be required if the guest is a minor.
- e. Access to all data on, taken from, or compiled using School District computers is subject to inspection and discipline. Users have no right to expect that School District information placed on users' personal computers, networks, Internet, and electronic communications systems is beyond the access of the School District. The School District reserves the right to legally access students' and employees' personal equipment for School District information.

2. Parental Notification and Responsibility

The School District will notify the parents about the School 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 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 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 is and is

not acceptable for their child(ren) to access through the School District's CIS system. Parents are responsible for monitoring their children'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 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 School District shall not be responsible for material that is retrieved through the Internet, or the consequences that may result from them. The School District shall not be responsible for any unauthorized financial obligations, charges or fees resulting from access to the School District's CIS systems. In no event shall 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 are in effect any time School District resources are accessed whether on School 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 or student uses their own equipment.

Students must also comply with the School District's Electronic Devices Policy located in the Student Code of Conduct.

a. General Prohibitions

Users are prohibited from using School District CIS systems to:

- (1) Communicate about non-work or non-school related communications unless the employees' use comports with this policy's definition of incidental personal use.
- (2) Send, receive, view, download, access or transmit material that is harmful to minors, indecent, obscene, pornographic, child pornographic, terroristic, or advocates the destruction of property.
- (3) Send, receive, view, download, access or transmit inappropriate matter and 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) Cyberbullying 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.
- (7) Send terroristic threats, hateful mail, harassing communications, discriminatory remarks, and offensive or inflammatory communications.
- (8) Participate in unauthorized Internet Relay Chats, 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.

- (9) Facilitate any illegal activity.
- (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).
- (11) 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 of 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 are defined as offering or providing goods or services or purchasing goods or services for personal use. School District acquisition policies will be followed for School District purchase of goods or supplies through the School District system.
- (12) Political lobbying or union activities unless authorized by administration.
- (13) 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 Section 8 Copyright Infringement in this Policy and the School District’s Copyright Policy for additional information.
- (14) 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 Chief Information Officer or designee.
- (15) 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. Employees and students must use School District approved encryption to protect the confidentiality of sensitive or critical information in the School District's approved manner.

- (16) 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.
- (17) Violate the privacy or security of electronic information.
- (18) Use the systems to 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.
- (19) Sending unsolicited commercial electronic mail messages, also known as spam.
- (20) Posting personal or professional web pages without administrative approval.
- (21) Post anonymous messages.
- (22) Use the systems for a job search.

b. Access and Security Prohibitions

Users must immediately notify the Chief Information Officer and/or designee if they have identified a possible security problem. Users must read, understand, provide a signed acknowledgement form(s), 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 School 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 another.

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 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.
- (5) 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.
- (6) 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.
- (7) Transmitting electronic communications anonymously or under an alias unless authorized by the School District.

c. 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 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 a person's

computer, or “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.
- (4) Attempting to alter any School District computing or networking components (including, but not limited to file servers, bridges, routers, or hubs) without authorization or beyond one’s level of authorization.
- (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 using unauthorized games, programs, files, or other electronic media, including, but not limited to, downloading music files.
- (8) Intentionally damaging or destroying the integrity of the School District’s electronic information.
- (9) Intentionally destroying the School District’s computer hardware or software.
- (10) Intentionally disrupting the use of the CIS systems.
- (11) Damaging the School District’s CIS systems, networking equipment through the users’ negligence or deliberate act.
- (12) 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 Guidelines

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

- a. 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 parent 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 parent 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 and guidelines, including the copyright policy.
- 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 policy, or the law may be discovered by routine maintenance and monitoring of the School District system, or any method stated in

this policy, or pursuant to any legal means.

- b. The School 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. Students and employees should not have the expectation of privacy in their use of the School District's CIS systems, and other School District technology, even when used for personal reasons. Further, the School District reserves the right, but not the obligation, to legally access any personal technology device of students and employees brought onto the School District's 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) to insure compliance with this policy and other School District policies, 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

- a. Federal laws, cases, and guidelines pertaining to copyright will govern the use of material accessed through the School District resources. Users will make a standard practice of requesting permission from the holder of the work and complying with license 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.
- 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 their own risk and assumes all liability.
- c. 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 School District's computers is expressly prohibited. This includes all forms of licensed software – shrink-wrap, clickwrap, browwrap, and electronic software downloaded from the Internet.

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

9. Selection of Material

- a. Board 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 will select material that is appropriate in light of 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.

10. School District Web Site

The School District will establish and maintain a Web Site and will develop and modify its Web pages that will present information about the School District under the direction of the Chief Information Officer and/or designee. Publishers must comply with the School District's Web Site Development Policy.

11. Safety & Privacy

- a. To the extent legally required, users of the School 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 Information Officer and/or designee.

- b. 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 School 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/video and Internet access to take pictures of anything, including but not limited to, persons, places, and documents relevant to the Colonial School 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 School District unless legitimately authorized to do so).
- c. Student users will agree not to meet with someone they have met online unless they have parent consent.

12. 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. Students and employees must be aware that violations of this policy or other policies, or 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, 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 School 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.
- b. 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.

- c. Violations as described in this policy may be reported to the School District, appropriate legal authorities, whether the ISP, local, state, or federal law enforcement. 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 is subject to discipline.

Disclaimer

The District makes no warranties of any kind, whether express or implied, for the service it is providing. The District is not responsible, and will not be responsible, for any damages, including loss of data resulting from delays, non-deliveries, missed deliveries or service interruption. Use of any information obtained through the use of the District's computers is at the user's risk.

The District disclaims responsibility for the accuracy or quality of information obtained through the Internet or E-mail.

Charges

The District assumes no responsibility or liability for any charges incurred by a user unless authority is expressly given by the Chief Information Officer. Under normal procedures governing use of the District's technology, there will be no cost incurred. Should a user incur charges without express authorization, such charges will be the user's responsibility.

Section: Operations
Title: Acceptable Use of the Computers, Network, Internet, Electronic Communications and Information Systems Policy
Adopted: April 21, 2005
Revised: August 19, 2010