ALLENTOWN SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF COMMUNICATIONS AND INFORMATION (CIS) SYSTEMS

ADOPTED: 6/21/07

REVISED: 12/16/10

815. ACCEPTABLE USE OF COMMUNICATIONS AND INFORMATION (CIS) SYSTEMS

Section 1. Purpose

The Allentown School District ("school district") provides employees, students, and Guests ("users") with hardware, software, and access to the school district's electronic communication system and network, which includes internet access, whether wired, wireless, virtual, cloud, or by any other means. Guests include, but are not limited to, visitors, workshop attendees, volunteers, adult education staff, students, School Board members, independent contractors, vendors, and school district consultants. Computers, network, Internet, electronic communications, information systems, databases, files, software, and media, collectively called "CIS" systems, provide vast, diverse and unique resources. The Board of School Directors will provide access to the school district's CIS systems for Users if there is a specific school district related purpose to access information, to research; to collaborate, to facilitate learning and teaching; and to foster the educational purpose and mission of the school district. For Users, the School district's CIS systems must be used for educational purposes and performance of school district job duties in compliance with this policy and accompanying Administrative Regulation #815. For employees, *Incidental personal use* (as defined in this policy) of school district computers is permitted. However, they should have no expectation of privacy in anything they create, store, send, receive, or display on or over the School district's CIS systems, including their personal files, or any of their use. Students may only use the CIS systems for educational purposes. CIS systems may include school district computers which are located or installed on school district property, at school district events, connected to the school district's network and/or systems, or when using its mobile computing equipment, telecommunication facilities in unprotected areas or environments, directly from home, or indirectly through another Internet Service Provider ("ISP"), and if relevant, when users bring and use their own personal computers or personal electronic devices, and if relevant, when users bring and use another entity's computer or electronic devices to a school district location, event, or connect to a school district network. If users bring personal computers or personal technology devices onto the school district property, to school district events, or connect them to the school district's network and systems, and if the school district reasonably believes the personal computers and personal electronic devices contain school district information or contain information that violates a school district policy or administrative regulation, the legal rights of the school district or another person, or involves significant harm to the school district or another person, or involves a criminal activity, the personal computers or personal electronic devices may be legally accessed to insure compliance with this policy and accompanying administrative regulation, other School district policies, regulations, rules, procedures, ISP terms, and local, state and federal laws. Users may not use their personal computers and personal technology devices to access the School district's intranet, internet or any other CIS system unless approved by the Superintendent, and/or designee. The school district intends to strictly protect its CIS systems against 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 accompanying administrative regulation, and to immediately report any violations or suspicious activities to the Superintendent, and/or designee. Conduct otherwise will result in actions further described in the Consequences for Inappropriate, Unauthorized and Illegal Use section found in the last section of this policy, and provided in other relevant school district policies and regulations, rules and procedures.

Section 2. Definitions

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:

1. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
2. 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,
3. Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct. 20 U.S.C. § 6777; 18 U.S.C.§2256(8), 47 U.S.C. § 254(h)(7)(F)

Under Pennsylvania law, any person who intentionally views or knowingly possesses or controls any book, magazine, pamphlet, slide, photograph, film, videotape, computer depiction or other material depicting a child under the age of eighteen (18) years engaging in a prohibited sexual act or in the simulation of such act. 18 Pa. C.S.A. §6312(d); 24 P.S. § 4603

Computer – includes any school district owned, leased or licensed or user-owned personal hardware, software, or other technology device used on school district premises or at school district events, or connected to the school district network, containing school district programs or school district or student data (including images, files, and other information) attached or connected to, installed in, or otherwise used in connection with a Computer. For example, *Computer* includes, but is not limited to, the school district's and Users': desktop, notebook, powerbook, tablet PC, iPad, Kindle, eBook Reader, or laptop computers, printers, facsimile machine, cables, modems, and other peripherals, specialized electronic equipment used for students' special educational purposes, global position system ("GPS") equipment, RFID, personal digital assistants ("PDAs"), iPods, MP3 players, thumb drives, cell phones (with or without internet access and/or recording and/or camera/video and other capabilities and configurations), telephones, mobile phones or wireless devices, two-way radios/telephones, beepers, paging devices, laser pointers and attachments, Pulse Pens, and any other such technology developed.
20 U.S.C. § 6777 (e); 18 U.S.C. § 2256(6), Policy #237, Electronic Devices.

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, photo optical or photoelectronic facilities for the transmission/transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature, wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications. Examples include, without limitation, the internet, intranet, voice mail services, electronic mail services,

tweeting, text messaging, instant messaging, GPS, PDAs, facsimile machines, cell phones (with or without internet access and/or electronic mail and/or recording devices, cameras/video, and other capabilities and configurations).

Educational Purpose - includes use of the CIS systems for classroom activities, professional or career development, and to support the school district's curriculum, policies, regulations, rules, procedures, and mission statement.

Harmful to Minors - under federal law, any picture, image, graphic image file or other visual depictions that:

1. Taken as a whole, with respect to minors, appeals to the prurient interest in nudity, sex, or excretion;

2. 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,

3. Taken as a whole lacks serious literary, artistic, political, educational or scientific value as to Minors. 20 U.S.C. § 6777(e)(6); 47 U.S.C. § 254(h)(7) (G).

Under Pennsylvania law, that quality of any depiction or representation, in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it:

1. Predominantly appeals to the prurient, shameful, or morbid interest of minors;

2. Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable for minors; and,

3. Taken as a whole, lacks serious literary, artistic, political, educational or scientific value for minors. 18 Pa. C.S.A. § 5903 (e)(6); 24 P.S. § 4603.

Inappropriate Matter - includes, but is not limited to visual, graphic, video, text and any other form of indecent, obscene, pornographic, child pornographic, or other material that is harmful to minors, sexually explicit, or sexually suggestive. Examples include, taking, disseminating transferring, or sharing obscene, pornographic, lewd, or otherwise illegal images or photographs, whether by electronic data transfer or otherwise (such as sexting, e-mailing, texting, among others). Others include, 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, flagging, terroristic material, and advocating the destruction of property.

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, accompanying administrative regulations, and all other applicable school district policies, regulations, procedures and rules, as well as ISP terms, local, state and federal laws, and must not damage the school district's CIS

systems.

Minor - for purposes of compliance with the federal Children's Internet Protection Act ("FedCIPA"), an individual who has not yet attained the age of seventeen (17). For other purposes, minor shall mean the age of minority as defined in the relevant law. 20 U.S.C. § 6777 (e); 47 U.S.C. § 254 (h)(7)(D); 18 U.S.C. § 2256; 18 Pa.C.S.A. § 5903(e).

Obscene - under federal law, analysis of the material meets the following elements:

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

2. 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,

3. Whether the work taken as a whole lacks serious literary, artistic, political, educational, or scientific value. 18 U.S.C. § 1460; 20 U.S.C. § 6777(e; 47 U.S.C. § 254(h)(7)(E).

Under Pennsylvania law, any material or performance, if:

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

2. The subject matter depicts or describes in a patently offensive way, sexual conduct described in the law to be obscene; and,

3. The subject matter, taken as a whole, lacks serious literary, artistic, political, educational or scientific value. 18 Pa. C.S.A. § 5903(b); 24 P.S. § 4603.

Sexual Act and Sexual Contact - is defined at 18 U.S.C. § 2246(2), at 18 U.S.C.§ 2246(3), and at 18 Pa. C.S.A. § 5903. 18 U.S.C. § 2246; 18 Pa. C.S.A. § 5903 (e)(3); 20 U.S.C. § 6777(e); 47 U.S.C. § 254(h)(7)(H).

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. 47 U.S.C. § 254(h)(7)(I); 24 P.S. § 4606.

Visual Depictions – includes undeveloped film and videotape, and data stored on a computer disk or by electronic means which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format, but does not include mere words. 18 U.S.C. § 1460 (b); 18 Pa.C.S.A. § 2256.

Section 3. Authority

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. The school district reserves the right to deny access to prevent 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. 47 U.S.C. § 254(l); 24 P.S. § 510; 24 P.S. § 4604. It is often necessary to access users' accounts in order to perform routine maintenance and security tasks. System administrators have the right to access by interception, and access the stored communication of user accounts for any reason in order to uphold this policy, accompanying administrative regulation, the law, and to maintain the system. USERS SHOULD HAVE NO EXPECTATION OF PRIVACY IN ANYTHING THEY CREATE, STORE, SEND, RECEIVE, OR DISPLAY ON OR OVER THE SCHOOL DISTRICT'S CIS SYSTEMS, INCLUDING THEIR PERSONAL FILES OR ANY OF THEIR USE OF THE SCHOOL DISTRICT'S CIS SYSTEMS. The school district reserves the right to record, check, receive, monitor, track, log access and otherwise inspect any or all CIS systems use and to monitor and allocate fileserver space. Users of the school district's CIS systems who transmit or receive communications and information shall be deemed to have consented to having the content of any such communications recorded, checked, received, monitored, tracked, logged, accessed, and otherwise inspected or used by the School district, and to monitor and allocate fileserver space. Passwords and message delete functions do not restrict the school district's ability or right to access such communications or information. The school district reserves the right to restrict access to any internet sites or functions it may deem inappropriate through general policy, software blocking or online server blocking. Specifically, the school district operates and enforces technology protection measure(s) that block or filter online activities of minors on its computers used and accessible to adults and students so as to filter or block inappropriate matter as defined in this policy o n the internet. The technology protection measure must be enforced during use of computers with internet access. Measures designed to restrict adults' and minors' access to material harmful to minors may be disabled to enable an adult or a student (who has provided written consent from a parent or guardian) to access *bona fide* research, not within the prohibitions of this policy, its accompanying administrative regulation, 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 and/or its administrative regulation is denying a student or adult to access material will be enforced by an administrator, supervisor, or their designee, upon the receipt of written consent from a parent or guardian for a student, and upon the written request from an adult presented to the Director of Information Technology. The school district has the right, but not the duty, to inspect, review, or retain electronic communication created, sent, displayed, received or stored on and over its CIS systems; to monitor, record, check, track, log, access or otherwise inspect; and/or to report all aspects of its CIS systems use. This includes any user's personal computers, networks, internet, electronic communication systems, computers, databases, files, software, and media that they bring onto school district property, or to school district events, that are connected to the school district network, or when using the school district's mobile commuting equipment, telecommunications facilities in unprotected areas or environments, directly from home, or indirectly through another ISP, and if relevant, when users bring and use another entity's computer or electronic device to a school district location, event, or connect it to a school district network and/or systems, and/or that contain school district programs, or school district or users' data or information, all pursuant to the law, in order to insure compliance with this policy, its administrative regulation, and other school district policies, regulations, rules, and procedures, ISP terms, and local, state, and federal laws, to protect the school district's resources, and to comply with the law. 47 U.S.C. § 254(l); 24 P.S. § 510; 24 P.S. § 4604; 20 U.S.C. § 6777(c); 24 P.S. § 4610; 20 U.S.C. § 6777(c); 24 P.S. § 4610.

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:

1. Highest - uses that directly support the education of the students;

2. Medium - uses that indirectly benefit the education of the student;

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

4. Forbidden - all activities in violation of this policy, its accompanying administrative regulation, other school district policies, regulations, rules, procedures, ISP terms, and local, state or federal law.

The school district additionally reserves the right to:

1. Determine which CIS systems services will be provided through school district resources;

2. Determine the types of files that may be stored on school district file servers and computers;

3. View and monitor network traffic, fileserver space, processor, and system utilization, and all applications provided through the network and electronic communications systems, including e-mail, text messages, and other electronic communications;

4. Remove excess e-mail and other electronic communications or files taking up an inordinate amount of fileserver space after a reasonable time; and,

5. Revoke User privileges, remove user accounts, or refer to legal authorities, and or school district authorities when violation of this and any other applicable school district policies, regulations, rules, and procedures occur or ISP terms, or local, state or federal law is violated, including, but not limited to, those governing network use, copyright, security, privacy, employment, vendor access, and destruction of School district resources and equipment.

Section 4. Delegation of Responsibility
The Superintendent is granted the authority to create an administrative regulation to accompany this policy. The administrative regulation must include, among other sections: Prohibitions (*General Prohibitions, Access and Security Prohibitions,* and *Operational Prohibitions)*, Content Guidelines, Due Process, Search and Seizure, and Selection of Material. This policy must be incorporated into the administrative regulation. The Superintendent is also granted the authority to create an administrative regulation that specifically addresses teacher-student communication when social networking tools are used. Due to the nature of the internet as a global network connecting thousands of computers around the world, inappropriate matter can be accessed through the network and electronic communications systems. Because of the nature of the technology that allows the internet to operate, the school district cannot completely block or filter access to these resources. Accessing these and similar types of resources may be considered an unacceptable use of school district resources and will result in actions explained further in the consequences for inappropriate, unauthorized and illegal use section found in the last section of this policy and in other relevant school district policies. The school district must publish a current version or summary of this policy so that all users are informed of their

responsibilities. A summary of this policy and *CIS Acknowledgement and Consent Form* must be provided to all users, who must sign the school district's *CIS Acknowledgement and Consent Form.* Users must be capable and able to use the school district's CIS systems and software relevant to the employee's responsibilities. The Superintendent, and/or designee, will serve as the coordinator to oversee the school district's CIS systems and will work with other regional or state organizations as necessary to educate users, approve activities, provide leadership for proper training for all users in the use of the CIS systems and the requirements of this Policy and its accompanying administrative regulation, establish a system to insure adequate supervision of the CIS systems, maintain executed user *CIS Acknowledgement and Consent Forms*, and interpret and enforce this policy and its accompanying administrative regulation. The Superintendent, and/or designee, will establish a process for setting-up individual and class accounts, set quotas for disk usage on the system, establish Record Retention and Records Destruction Policies and Records Retention Schedule to include electronically stored information, and establish the school district virus protection process. Unless otherwise denied for cause, student access to the CIS systems resources must be through supervision by the professional staff. Administrators, teachers and staff have the responsibility to work together to help students develop the skills and judgment required to make effective and appropriate use of the resources. All users have the responsibility to respect the rights of all other users within the School district and School district CIS systems, and to abide by the policies, regulations, rules, and procedures established by the school district, as well as ISP terms, and local, state and federal laws. The Superintendent, and/or designee, has the responsibility to educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response. 47 U.S.C. § 254 (5)(B)(iii); 24 P.S. § 1303.1-A; Policy #249, Bullying/Cyberbullying.

Section 5. Guidelines

Access To The CIS Systems

The CIS systems accounts of users must be used only by authorized owners of the accounts and only for authorized purposes. An account must be made available according to a procedure developed by appropriate school district authorities.

CIS System. This policy, its accompanying administrative regulation, as well as other relevant school district policies, regulations, rules, and procedures, will govern use of the school district's CIS systems for users.

Types of Services include, but are not limited to:

1. Internet - School district employees, students, and guests will have access to the internet through the school district's CIS systems, as needed.

2. E-Mail and Text Messaging - School district employees may be assigned individual e-mail and text message accounts for work related use, as needed. Students may be assigned individual e-mail accounts, as necessary, by the Director of Information Technology, and/or designee, at the recommendation of the teacher who will also supervise the students' use of the e-mail service. Students may not be assigned text message accounts.

3. Guest Accounts – Guests may receive an individual internet account with the approval of the Superintendent, and/or designee, if there is a specific school district-related purpose requiring such access. Use of the CIS systems by a guest must be specifically limited to the school district-related purpose and comply with this policy, its accompanying administrative regulation, and all

other school district policies (including the Vendor Access Policy), regulations, rules and procedures, as well as ISP terms, local, state and federal laws, and may not damage the school district's CIS systems. A school district *CIS Acknowledgment and Consent Form* must be signed, and if the guest is a minor, a parent's written signature is required.

4. Blogs - Employees may be permitted to have school district-sponsored blogs, after they receive training, and the approval of the Superintendent, or designee. All bloggers must follow the rules provided in this policy, its accompanying administrative regulation, and other applicable policies, regulations, rules and procedures of the school district, as well as ISP terms, and local, state, and federal laws.

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

Parental Notification and Responsibility

The school district will notify the parents/guardians about the school district's CIS systems and the policies, and regulations governing their use. This policy, and its accompanying regulation contain 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 wide range of social values in student use of the internet. Further, the school district recognizes that parents/guardians bear primary responsibility for transmitting their particular set of family values to their children. The school district will encourage parents to specify to their children what material and matter is and is not acceptable for their children to access through the school district's CIS system.

School District Limitation of Liability

The school district makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the school district's CIS systems will be error-free or without defect. The school district does not warrant the effectiveness of internet filtering. The electronic information available to users does not imply endorsement of the content by the school district, nor is the school district responsible for the accuracy or quality of the information obtained through or stored on the CIS systems. The school district will not be responsible for any damage users may suffer, including but not limited to, information that may be lost, damaged, delayed, misdelivered, or unavailable when using the CIS systems. The school district will not be responsible for material that is retrieved through the internet, or the consequences that may result from them. The school district will not be responsible for any unauthorized financial obligations, charges or fees resulting from access to the school district's CIS

systems. In no event will the school district be liable to the user for any damages whether direct, indirect, special or consequential, arising out of the use of the CIS systems.

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 in the accompanying administrative regulation #815. The school district reserves the right to determine if any activity not appearing in the lists constitutes an acceptable or unacceptable use of the CIS systems. The prohibitions are in effect any time school district resources are accessed whether on school district property, at school district events, connected to the school district's network, when using mobile computing equipment, telecommunication facilities in unprotected areas or environments, directly from home, or indirectly through another ISP, and if relevant, when a user uses their own equipment. Students must also comply with the school district's Policy # 237, Electronic Devices.

Copyright Infringement and Plagiarism

Federal laws, cases, policies, regulations, and guidelines pertaining to copyright will govern the use of material accessed through school district resources. (See School District Policy #815). Users will make a standard practice of requesting permission from the holder of the work, comply with the Fair Use Doctrine, and/or complying with license agreements. Employees will instruct users to respect copyrights, request permission when appropriate, and comply with the Fair Use Doctrine and/or with license agreements. 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. Violations of copyright law include, but are not limited to, making unauthorized copies of any copyrighted material (such as commercial software, text, graphic images, audio and video recording), distributing copyrighted materials over Computer networks, remixing or preparing mash-ups, and deep-linking and framing into the content of others' websites. Further, the illegal installation of copyrighted software or files for use on the School district's Computers is expressly prohibited. This includes all forms of licensed software -- shrink-wrap, clickwrap, browse-wrap, and electronic software, downloaded from the internet. No one may circumvent a Technology Protection Measure that controls access to a protected work unless they are permitted to do so by law. No one may manufacture, import, offer to the public, or otherwise traffic in any technology, product, service, device, component or part that is produced or marketed to circumvent a technology protection measure to control access to a copyright protected work. 17 U.S.C. § 1202. school district guidelines on plagiarism will govern use of material accessed through the school district's CIS systems. Users must not plagiarize works that they find. Teachers will instruct students in appropriate research and citation practices. Users understand that use of the school district's CIS systems may involve the school district's use of plagiarism analysis software being applied to their work. Policy #814,Copyrighted Works.

School District Website

The school district has established and maintains a website and will develop and modify its web pages that will present information about the school district under the direction of the Superintendent, and/or designee. Publishers must comply with this policy, its accompanying administrative regulation, and other school district policies, regulations, rules, and procedures, ISP terms, and local, state, and federal laws. The school district may limit its liability by complying with the Digital Millennium Copyright Act's safe harbor notice and takedown provisions. 17 U.S.C. § 512.

Blogging
If an employee, student or guest creates a blog with their own resources and on their own time, the employee, student or guest may not violate the privacy rights of employees and students, may not use school district personal and private information/data, images and copyrighted material in their blog, and may not disrupt the school district. Conduct otherwise will result in actions further described in the Consequences for Inappropriate, Unauthorized and Illegal Use section of this policy, its accompanying administrative regulation, and provided in other relevant school district policies, regulations, rules, and procedures.

Safety and Privacy
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 unwelcomed communications must immediately send or take them to the Superintendent, and/or designee. Users must not post unauthorized personal contact information about themselves or other people on the CIS systems. Users may not steal another's identity in any way, may not use spyware, cookies, or other program code, and may not use school district or personal technology or resources in any way to invade one's privacy. Additionally, users may not disclose, use or disseminate confidential and personal information about students or employees. Examples include, but are not limited to, revealing biometric data, student grades, social security numbers, dates of birth, home addresses, telephone numbers, school addresses, work addresses, credit card numbers, health and financial information, evaluations, psychological reports, educational records, and resumes or other information relevant to seeking employment at the school district by using a PDA, iPhone, Blackberry, cell phone (with or without camera/video) and/or other Computer, unless legitimately authorized to do so. If the school district requires that data and information to be encrypted Users must use school district authorized encryption to protect their security. Student users must agree not to meet with someone they have met online unless they have parental consent. 47 U.S.C. § 254.

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, and its accompanying administrative regulation, other school district policies, regulations, rules, and procedures, ISP terms, and local, state and federal laws. Users must be aware that violations of this policy, its accompanying administrative regulation, or other policies, regulations, rules, and procedures, or for unlawful use of the CIS systems, may result in loss of CIS access and a variety of other disciplinary actions, including but not limited to, warnings, usage restrictions, loss of privileges, position reassignment, oral or written reprimands, student suspensions, employee suspensions (with or without pay), dismissal, expulsions, breach of contract, and/or legal proceedings on a case-by-case basis. This policy, and its accompanying administrative regulation, incorporate all other relevant school district policies, such as, but not limited to, the student and professional employee discipline policies, Code of Student Conduct, copyright, property, curriculum, terroristic threat, vendor access, and harassment policies. Users are responsible for damages to computers, the network, equipment, electronic communications systems, and software resulting from accidental, negligent, deliberate, and willful acts. Users will also be responsible for incidental or unintended damage resulting from negligent, willful or deliberate violations of this policy, accompanying administrative regulation, other school district policies, regulations, rules, and procedures, ISP terms, and local, state, and federal laws. For example, users will be responsible for payments related to lost or stolen computers and/or school district equipment, and recovery and/or breach of the data contained on them. Violations as described in this policy, and its accompanying

administrative regulation, other school district policies, regulations, rules, and procedures may be reported to the school district, and to appropriate legal authorities, whether the ISP, local, state, or federal law enforcement, and may constitute a crime under state and/or federal law, which may result in arrest, criminal prosecution, and lifetime inclusion on a sexual offenders registry. The school district will cooperate to the extent legally required with authorities in all such investigations. Vandalism will result in cancellation of access to the school district's CIS systems and resources and is subject to discipline. Any and all costs incurred by the school district for repairs and/or replacement of software, hardware and data files and for technological consultant services due to any violation of this policy, its accompanying regulation, other school district policies, regulations, rules, and procedures, or ISP terms, or federal, state, or local law, shall be paid by the user who caused the loss. Policies #317, Administrative Employee Disciplinary Procedures, Policy #417, Professional Employee Disciplinary Procedures, Policy # 517, Classified Employee Disciplinary Procedures.