Book	Policy Manual
Section	300 Employees
Title	Ethical Behavior of District Staff
Number	300
Status	Active
Legal	24 P.S. 510 Pol. 317 Pol. 317.1 Pol. 319
Adopted	September 8, 2016

Purpose

The Board believes that high standards of ethical behavior for administrative, professional and support employees are essential and compatible with their faith in the power of public education and committment to the preservation and strengthening of the public schools. To this end, the Board adopts the following policy guidelines.

Guidelines

The employee shall uphold the honor and dignity of his/her position in all his/her actions and interactions with students, district and school staff, Board members and the public.

The employee shall obey local, state and federal laws; hold him/herself to high ethical and moral standards; and model loyalty to his/her country and to the cause of democracy and liberty.

The employee shall accept the responsibility throughout his/her career to master and contribute to the growing body of specialized knowledge, concepts and skills which are inherent to success in his/her position.

The employee shall strive to provide the finest possible educational experiences and opportunities to all persons in the district.

The employee shall seek to preserve and enhance the prestige and status of his/her position in the school district.

The employee shall carry out in good faith all policies duly adopted by the Board, the regulations and laws of the Commonwealth and federal authorities, and render professional service to the best of his/her ability.

The employee shall honor the public trust of his/her position above any economic or social rewards.

The employee shall not permit considerations of private gain nor personal economic interest or gain to effect the discharge of his/her responsibilities.

The employee shall recognize that public schools are the public's business and seek to keep the public fully and honestly informed about their schools as permitted in Board policy and applicable laws and regulations, and to work with students, parents/guardians, other staff and the community to promote excellent opportunities for achievement and success.

Book	Policy Manual
Section	300 Employees
Title	Tobacco
Number	323
Status	Active
Legal	1. 35 P.S. 1223.5 2. 20 U.S.C. 7183 3. 24 P.S. 1302.1-A 4. 24 P.S. 1303-A 5. 22 PA Code 10.2 6. 22 PA Code 10.22 7. 18 Pa. C.S.A. 6305 8. Pol. 805.1 9. 35 P.S. 637.3 10. 35 P.S. 637.6 11. Pol. 317 20 U.S.C. 7181 et seq
Adopted	November 10, 2016

Purpose

The Board recognizes that tobacco presents a health and safety hazard that can have serious consequences for the user and the nonuser and the safety of the schools.

Definition

For purposes of this policy, **tobacco** includes a lighted or unlighted cigarette, cigar, pipe, other smoking product or material, chewing tobacco and all forms of smokeless tobacco, as well as look-alike items/devices including but not limited to electronic cigarettes.

Authority

The Board prohibits tobacco use or sale of tobacco as defined in this policy by administrative, professional and support employees in a school building; on any property owned, leased or controlled by the school district; and on buses, vans or other vehicles owned, leased or controlled by the school district, including contracted transportation services.[1][2]

Additonally, the Clean Indoor Air Act provides that an individual may not engage in smoking in a public place.[9]

The Board prohibits tobacco use or sale of tobacco as defined in this policy by district employees while performing assigned duties at any school-sponsored activity held off school property.[1]

The district shall annually notify employees about the Board's tobacco policy through the use of posted notices, via the district's website, and/or other efficient methods.[1]

Guidelines

The Superintendent or designee may report incidents involving the sale of tobacco to minors by employees on school property, at any school-sponsored activity or on a conveyance providing transportation to or from a school or school-sponsored activity to the local police department that has jurisdiction over the school's property, in accordance with state law and regulations, the procedures set forth in the memorandum of understanding with local law enforcement and Board policies.[3][4][5][6][7][8]

In accordance with state law, the Superintendent shall annually, by July 31, report incidents of possession, use or sale of tobacco on school property to the Office for Safe Schools on the required form.[4][8]

Any employee in violation of this policy risks being in violation of state and federal law and the possibility of facing criminal penalties, civil penalties, local penalties, and state penalties.[1][2][10]

Violation of this policy may also result in disciplinary action, up to and including dismissal.[11]

Book	Policy Manual
Section	300 Employees
Title	Confidential Information
Number	324.1
Status	Active
Legal	Pol. 113.4 Pol. 207 Pol. 216 Pol. 216.1 Pol. 324 Pol. 800 Pol. 801 Pol. 830
Adopted	November 10, 2016

Purpose

District employees, through and during the course of their employment, may be exposed to sensitive and/or confidential information about the school district, its employees and students.

It is the policy of the school district to ensure that sensitive and/or confidential information concerning the operations, activities, and business affairs of the district, as well as sensitive information regarding the district's employees and students, are kept confidential to the greatest extent possible.

Delegation of Responsibility

The district expects employees to protect the interests of the district and its employees and students by restricting the use and disclosure of all information relating to the district's affairs or personal matters pertaining to the district's employees or students, and all documents containing such information, to within the school district, unless specifically approved for outside disclosure, or already known by or readily available to the public. Employees shall also be responsible for the internal security of such information, and shall only disclose such information internally on a need-to-know basis. When in doubt, employees shall consider information confidential.

Employees will be asked to sign a receipt and acknowledgement form at the time of hire and may be asked periodically throughout their term of employment to acknowledge their awareness of this policy and to reaffirm their committment to comply with it. This policy shall continue to apply to former employees who had access to confidential information during the course of their employment with the district.

Employees with questions about handling confidential information should contact their immediate supervisor.

Book	Policy Manual
Section	300 Employees
Title	Dress and Grooming
Number	325
Status	Active
Legal	1. 24 P.S. 510 2. Pol. 345 3. Pol. 317
Adopted	December 8, 2016

Authority

Administrative, professional and support employees set an example in dress and grooming for students and the school community. Employees' dress should reflect their professional status and encourage respect for authority in order to have a positive influence on the district's programs and operations.

The Board has the authority to specify reasonable dress and grooming requirements, within law, for all district employees to prevent an adverse impact on the educational programs and district operations.[1]

When assigned to district duties, employees shall be physically clean, neat, well-groomed and dressed in a manner consistent with assigned job responsibilities.

Employees shall be groomed so that their hair style does not cause a safety or health hazard.

Designated support employees shall be required to utilize safety gear when performing assigned duties and wear appropriate work uniforms or clothing as specified in the collective bargaining agreement.

The district shall provide each employee with a photo identification badge, which shall be worn and readily visible when on duty, in accordance with Board policy.[2]

Delegation of Responsibility

If an employee feels that an exception to this policy would enable him/her to carry out assigned duties more effectively, a request should be made to the Superintendent or designee.

Guidelines

Violation of this policy may result in appropriate disciplinary action.[3]

Book	Policy Manual
Section	300 Employees
Title	Unlawful Harassment
Number	348
Status	Active
Legal	1. 43 P.S. 951 et seq 2. 20 U.S.C. 1681 et seq 3. 42 U.S.C. 2000e et seq 4. 42 U.S.C. 2000ff et seq 5. 29 CFR 1606.8 6. 29 CFR 1604.11 7. Pol. 104 8. Pol. 317
Adopted	February 9, 2017

Authority

The Board strives to provide a safe, positive working climate for its administrative, professional and support employees. Therefore, it shall be the policy of the district to maintain an employment environment in which harassment in any form is not tolerated.

The Board prohibits all forms of unlawful harassment of employees and third parties by all district students and staff members, contracted individuals, vendors, volunteers, and third parties in the schools. The Board encourages employees and third parties who have been harassed to promptly report such incidents to the designated administrators.[1][2][3][4][5]

The Board directs that complaints of harassment shall be investigated promptly, and corrective action taken when allegations are substantiated. Confidentiality of all parties shall be maintained, consistent with the district's legal and investigative obligations.

No reprisals nor retaliation shall occur as a result of good faith charges of harassment.

Definitions

For purposes of this policy, **harassment** shall consist of verbal, written, graphic or physical conduct relating to an individual's race, color, national origin/ethnicity, sex, age, disability, sexual orientation, religion or genetic information when such conduct:[4][5]

1. Is sufficiently severe, persistent or pervasive that it affects an individual's ability to perform job functions or creates an intimidating, threatening or abusive work environment.

2. Has the purpose or effect of substantially or unreasonably interfering with an individual's work performance.

3. Otherwise adversely affects an individual's employment opportunities.

For purposes of this policy, **sexual harassment** shall consist of unwelcome sexual advances; requests for sexual favors; and other inappropriate verbal, written, graphic or physical conduct of a sexual nature when:[6]

1. Acceptance of such conduct is made, explicitly or implicitly, a term or condition of an individual's continued employment.

2. Submission to or rejection of such conduct is the basis for employment decisions affecting the individual.

3. Such conduct is sufficiently severe, persistent or pervasive that it has the purpose or effect of substantially interfering with the employee's job performance or creating an intimidating, hostile or offensive working environment.

Examples of conduct that may constitute sexual harassment include but are not limited to sexual flirtations, advances, rumors, touching or propositions; verbal abuse of a sexual nature; sexually graphic or suggestive comments; sexually degrading words to describe an individual; jokes; pin-ups; calendars; objects; graffiti; drawings; pictures; written materials; innuendoes; references to sexual activities; overt sexual conduct or gestures; circulating or showing emails or websites of a sexual nature; or any conduct that has the effect of unreasonably interfering with a student's ability to work or learn or creates an intimidating, hostile or offensive learning or working environment.

Delegation of Responsibility

In order to maintain a work environment that discourages and prohibits unlawful harassment, the Board designates the Director of Human Resources as the district's Compliance Officer.[7]

The Compliance Officer shall publish and disseminate this policy and the complaint procedure at least annually to students, parents/guardians, employees, independent contractors, vendors, and the public. The publication shall include the position, office address and telephone number of the Compliance Officer.

The administration shall be responsible to provide training for students and district employees regarding unlawful harassment.

Each employee shall be responsible to maintain a working environment free from all forms of unlawful harassment.

The building principal or immediate supervisor shall be responsible to complete the following duties when receiving a complaint of unlawful harassment:

1. Inform the employee or third party of the right to file a complaint and the complaint procedure.

2. Notify the complainant and the accused of the progress at appropriate stages of the procedure.

3. Refer the complainant to the Compliance Officer if the building principal or immediate supervisoris the subject of the complaint.

Guidelines

Complaint Procedure – Employee/Third Party

Step 1 – Reporting

An employee or third party who believes s/he has been subject to conduct that constitutes a violation of this policy is encouraged to immediately report the incident to the building principal or immediate supervisor.

If the building principal or immediate supervisor is the subject of a complaint, the employee or third party shall report the incident directly to the Compliance Officer.

The complainant is encouraged to use the report form available from the building principal, immediate supervisor, or Compliance Officer, but oral complaints shall be acceptable. Oral complaints will be transcribed and must be signed by the complainant.

Step 2 – Investigation

Upon receiving a complaint of unlawful harassment, the building principal or immediate supervisor shall immediately notify the Compliance Officer. The Compliance Officer shall authorize the building principal or immediate supervisor to investigate the complaint, unless the building principal or immediate supervisor is the subject of the complaint or is unable to conduct the investigation.

The investigation may consist of individual interviews with the complainant, the accused, and others with knowledge relative to the incident. The investigator may also evaluate any other information and materials relevant to the investigation.

The obligation to conduct this investigation shall not be negated by the fact that a criminal investigation of the incident is pending or has been concluded.

Step 3 – Investigative Report

The building principal or immediate supervisor shall prepare and submit a written report to the Compliance Officer within fifteen (15) days, unless additional time to complete the investigation is required. The report shall include a summary of the investigation, a determination of whether the complaint has been substantiated as factual and whether it is a violation of this policy, and a recommended disposition of the complaint.

The complainant and the accused shall be informed of the outcome of the investigation, including the recommended disposition of the complaint.

Step 4 – District Action

If the investigation results in a finding that the complaint is factual and constitutes a violation of this policy, the district shall take prompt, corrective action to ensure that such conduct ceases and will not recur. District staff shall document the corrective action taken and, when not prohibited by law, inform the complainant.

Disciplinary actions shall be consistent with Board policies, administrative regulations and procedures, applicable collective bargaining agreements, and state and federal laws.

If it is concluded that an employee has knowingly made a false complaint under this policy, such employee shall be subject to disciplinary action.[8]

Appeal Procedure

1. If the complainant is not satisfied with a finding of no violation of the policy or with the recommended corrective action, s/he may submit a written appeal to the Compliance Officer within fifteen (15) days.

2. The Compliance Officer shall review the investigation and the investigative report and may also conduct a reasonable investigation.

3. The Compliance Officer shall prepare a written response to the appeal within fifteen (15) days. Copies of the response shall be provided to the complainant, the accused and the building principal or immediate supervisor who conducted the initial investigation.

348-Attach.doc (27 KB)

Book	Policy Manual
Section	300 Employees
Title	Drug and Substance Abuse
Number	351
Status	Active
Legal	1. 35 P.S. 780-101 et seq 2. 41 U.S.C. 8101 3. 24 P.S. 111 4. 41 U.S.C. 8103 5. 24 P.S. 527 6. 41 U.S.C. 8104 7. 24 P.S. 1302.1-A 8. 24 P.S. 1303-A 9. 22 PA Code 10.2 10. 22 PA Code 10.21 11. 35 P.S. 780-102 12. Pol. 805.1 13. Pol. 324 41 U.S.C. 8101 et seq Pol. 317
Adopted	February 9, 2017

Purpose

The Board recognizes that the misuse of drugs, alcohol and other controlled substances by administrative, professional and support employees is a serious problem with legal, physical and social implications for the whole school community and is concerned about the problems that may be caused by drug use by district employees, especially as the use relates to an employee's safety, efficiency and productivity.

The primary purpose and justification for any district action will be for the protection of the health, safety and welfare of students, staff and school property.

Definitions

Drugs - shall be defined as those outlined in the Controlled Substance, Drug, Device and Cosmetic Act.[1]

Conviction - a finding of guilt, including a plea of nolo contendere, an imposition of sentence, or both by any judicial body charged with the responsibility to determine violations of the federal or state criminal drug statutes.[2]

Criminal Drug Statute - a federal or state criminal statute involving the manufacture, distribution, dispensation, use or possession of a controlled substance.[2]

Drug-free Workplace - the site for the performance of work at which employees are prohibited from engaging in the unlawful manufacture, distribution, dispensation, possession or use of a controlled substance.[2]

Authority

The Board requires that each administrative, professional and support employee be given notification that, as a condition of employment, the employee will abide by the terms of this policy and notify the district of any criminal drug statute conviction for a violation occurring in the workplace immediately, but no later than seventy-two (72) hours, after such conviction.[3][4]

Any employee convicted of delivery of a controlled substance or convicted of possession of a controlled substance with the intent to deliver shall be terminated from his/her employment with the district.[5][1]

Delegation of Responsibility

A statement notifying employees that the unlawful manufacture, distribution, dispensation, possession, or use of a controlled substance is prohibited in the employee's workplace shall be provided by the Superintendent or designee and shall specify the actions that will be taken against the employee for violation of this policy, up to and including termination and referral for prosecution.[4][6]

Within ten (10) days after receiving notice of the conviction of a district employee, the district shall notify any federal agency or department that is the grantor of funds to the district.[4]

The district shall take appropriate personnel action within thirty (30) days of receiving notice against any convicted employee, up to and including termination, or require the employee to participate satisfactorily in a drug abuse assistance or rehabilitation program approved for such purposes by a federal, state or local health, law enforcement, or other appropriate agency.[4][6]

Employees may be suspended with or without pay pending completion of an investigation.

Employees undergoing counseling or treatment will not be exempt from the district's rules, Boardpolicy, procedures or disciplinary action.

All information obtained in the course of assistance, counseling, rehabilitation or treatment of employees with alcohol, drug, or controlled substance abuse problems shall be protected as confidential medical information and shall be kept separate from the employee's official personnel file.[13]

In establishing a drug-free awareness program, the Superintendent or designee shall inform employees about:[4]

1. Dangers of drug or substance abuse in the workplace.
2. Board's policy of maintaining a drug-free workplace.
3. Availability of drug counseling, drug rehabilitation, and employee assistance programs.
4. Penalties that may be imposed upon employees for drug or substance abuse violations occurring in the workplace.

The district shall make a good faith effort to continue to maintain a drug-free workplace through implementation of this policy.[4]

Guidelines

The Superintendent or designee shall immediately report incidents involving the possession, use or sale of a controlled substance or drug paraphernalia as defined in the Pennsylvania Controlled Substance, Drug, Device and Cosmetic Act by any employee while on school property, at any school-sponsored activity or on a conveyance providing transportation to or from a school or school-sponsored activity to the local police department that has jurisdiction over the school's property, in accordance with state law and regulations, the procedures set forth in the memorandum of understanding with local law enforcement and Board policies.[7][8][9][10][11][12]

In accordance with state law, the Superintendent shall annually, by July 31, report all incidents of possession, use or sale of controlled substances or drug paraphernalia to the Office for Safe Schools on the required form.[8][12]

Book	Policy Manual
Section	300 Employees
Title	Communication Devices, Cellular Telephones and Other Electronic Devices
Number	352
Status	Active
Legal	24 P.S. 510 Pol. 717 Pol. 815
Adopted	February 9, 2017

Purpose

The Board recognizes the need to ensure an environment that is safe and secure for employees, students and visitors. The Board also recognizes the need to provide employees reasonable access to technological resources.

Definition

For purposes of this policy, **communications device** shall be defined so as to include any portable two-way telecommunications device including, but not limited to, the following: cellular telephones (with or without cameras, the ability to text message, the ability to email, and/or the ability to access the Internet); walkie-talkies; other hand-held computing devices (such as tablets, smart phones, and similar devices); any portable electronic devices capable of storing, transmitting and/or receiving messages or images; and any new technology developed with similar capabilities.

Guidelines

The Board prohibits all employees from using any personal or district-issued communications device during work hours for any purpose unrelated to the employee's job duties, unless:

1. The employee is on an approved scheduled break and is in a lunch room, break room, or other area where s/he cannot be seen or overheard by students and/or guests on district property.

2. The employee is experiencing an emergency where there is a clear and present danger and the brief use of a communications device cannot be reasonably avoided. If an employee wishes to use a communications device in response to an emergency, the employee shall use discretion to ensure that the learning environment is not disrupted, to ensure that the propriety, quiet and order of the workplace is maintained, and/or to ensure the privacy of others.

3. The employee has been specifically directed to use a communications device by a supervisor.

District employees are expected to adhere to any and all state and local laws regarding the use of communications devices while operating district motor vehicles or machinery, or when operating nonschool district motor vehicles or machinery during the course of performing work-related duties.

The Board prohibits the taking, storing, disseminating, transferring, viewing, or sharing of obscene, pornographic, lewd, or otherwise illegal images or photographs, whether by electronic data transfer or other means, including but not limited to texting or emails. Such violations may constitute a crime under state and/or federal law, and the district may report and/or may be required to report such conduct to state and/or federal law enforcement and/or other agencies.

An employee may use a personal and/or district-issued communications device in connection with his/her job-related duties if:

1. The use of the communications device has been narrowly tailored to perform a specific job-related duty.
2. The use of the communications device is reasonable, as determined by the employee's direct supervisor, a building administrator and/or the Superintendent or designee.
3. The employee has received permission from his/her direct supervisor, a building administrator, and/or the Superintendent or designee.

Permission to use a personal and/or district-issued communcations device in connection with a job-related duty may be revoked at any time and for any reason.

If the employee is a classroom teacher, the employee is encouraged to identify and propose ways in which technology, including the use of communications devices, may be integrated into student instruction.

Delegation of Responsibility

The Superintendent or designee shall notify all employees about this policy.

The Superintendent or designee may develop administrative regulations to implement this policy.

Book	Policy Manual
Section	800 Operations
Title	Acceptable Use of Communications and Information Systems (CIS)
Number	815
Status	Active

Legal

1. 18 U.S.C. 2256
2. 20 U.S.C. 6777
3. 47 U.S.C. 254
4. 18 Pa. C.S.A. 6312
5. 24 P.S. 4603
6. 18 Pa. C.S.A. 5903
7. Pol. 103
8. Pol. 103.1
9. Pol. 104
10. Pol. 218.2
11. Pol. 248
12. Pol. 249
13. 18 U.S.C. 2246
14. 24 P.S. 4604
15. Pol. 218
16. Pol. 233
17. Pol. 317
18. 24 P.S. 4610
19. Pol. 226
20. Pol. 237
21. Pol. 800
22. 47 CFR 54.520
23. 24 P.S. 1303.1-A
24. Pol. 229
25. Pol. 610
26. Pol. 611
27. Pol. 612
28. Pol. 913
29. Pol. 814
30. Pol. 830
31. 17 U.S.C. 101 et seq
32. Pol. 816
33. Pol. 348

24 P.S. 4601 et seq

Pol. 220

Adopted May 11, 2017

Purpose

The district provides employees, students, and other authorized users (guests)with hardware, software, and access to the district's electronic communications systems and network, which includes Internet access, whether wired, wireless, virtual, cloud, or by any other means.

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 the district's 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 Superintendent or designee. Conduct otherwise will result in actions further described in this policy and provided in other relevant Board policies.

Definitions

The term child pornography is defined under both federal and state law.

Child pornography - under federal law, is 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][2][3]

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.

Child pornography - under state law, is 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.[4][5]

Computer - includes any district-owned, leased or licensed or user-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, the district's and user's: desktop, notebook, powerbook, tablet PC 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); 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.

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

Electronic communications systems/electronic communications - 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 photo electronic 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, but are not limited to, the Internet, intranet, voice mail services, electronic mail services, tweeting, text messaging, instant messages, GPS, PDAs, facsimile machines, and cell phones (with or without Internet access and/or electronic mail and/or recording devices, cameras/video, and other capabilities).

Guest - includes, but is not limited to, visitors, workshop attendees, volunteers, adult education staff, students, Board members, independent contractors, and school district consultants.

The term harmful to minors is defined under both federal and state law.

Harmful to minors - under federal law, is any picture, image, graphic image file or other visual depiction that:[2][3]

1. Taken as a whole, with respect to minors, appeals to a 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 contact, 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 or scientific value as to minors.

Harmful to minors - under state law, is any depiction or representation in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it:[5][6]

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.

Inappropriate matter - includes, but is not limited to visual, graphic, video, 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, violent, bullying, sexting, flagging, terroristic, and advocates the destruction of property.[7][8][9][10][11][12]

Incidental personal use - incidental personal use of district 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 Board policies, procedures and rules, as well as

Internet Service Provider (ISP) terms, local, state and federal laws, and must not damage the district's CIS systems.

Minor - for purposes of compliance with the federal Children's Internet Protection Act (CIPA), 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.[2][3]

Obscene - any material or performance, if:[5][6]

1. The average person applying contemporary community standards would find that the subject matter 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.

Sexual act and sexual contact - is defined at 18 U.S.C. § 2246 and at 18 Pa. C.S.A. § 5903. [6][13]

Technology protection measure - a specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography or harmful to minors.[3][14]

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, and data 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.[1]

Authority

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. The district, further, reserves the right to deny access to prevent unauthorized, inappropriate or illegal activity, and may revoke access privileges and/or administer appropriate disciplinary action. The 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.[15][16] [17]

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 access the stored communication of user accounts for any reason in order to uphold this policy, 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 district's CIS systems, including their personal files or any of their use of the district's CIS systems. The 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.

The Board shall establish a list of materials, in addition to those stated in law and defined in this policy, that are inappropriate for access by minors.[3]

The district reserves the right to restrict access to any Internet sites or functions it deems inappropriate through established Board policy, or the use of software and/or online server blocking. Specifically, the district operates and enforces a technology protection measure(s)

that blocks or filters access to inappropriate matter by minors on its computers used and accessible to adults and students. The technology protection measure shall be enforced during use of computers with Internet access.[2][3][14]

Upon request by students or staff, the Superintendent or designee shall expedite a review and may authorize the disabling of Internet blocking/filtering software to enable access to material that is blocked through technology protection measures but is not prohibited by this policy.[14]

Upon request by students or staff, building administrators may authorize the temporary disabling of Internet blocking/filtering software to enable access for bona fide research or for other lawful purposes. Written permission from the parent/guardian is required prior to disabling Internet blocking/filtering software for a student's use. If a request for temporary disabling of Internet blocking/filtering software is denied, the requesting student or staff member may appeal the denial to the Superintendent or designee for expedited review.[2][18]

The district has the right, but not the duty, to inspect, review, or retain electronic communications 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, databases, files, software, and media that they bring onto district property, or to district events, that were connected to the district network, and/or that contain district programs, or district or user data or information, all pursuant to the law, in order to ensure compliance with this policy and other Board policies, to protect the district's resources, and to comply with the law.[19][20]

The district reserves the rights to restrict or limit usage of lower priority CIS systems and computer use when network and computing requirements exceed available capacity according to the following priorities:

1. Highest - use that directly supports the education of students.
2. Medium - use that indirectly benefits the education of students.
3. Lowest - use that includes reasonable and limited educationally-related employee interpersonal communications and employee-limited incidental personal use.
4. Forbidden - all activities in violation of this policy and local, state or federal law.

The district additionally reserves the right to:

1. Determine which CIS systems services will be provided through district resources.
2. Determine the types of files that may be stored on district fileservers 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 email.
4. Remove excess email or files taking up an inordinate amount of fileserver disk space after a reasonable time.

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

Delegation of Responsibility

The district shall inform staff, students, parents/guardians and other users about this policy through employee and student handbooks, posting on the district website, and by other appropriate methods. A copy of this policy shall be provided to parents/guardians, upon written request.[14]

Users of district networks or district-owned equipment shall, prior to being given access or being issued equipment, sign user agreements acknowledging awareness of the provisions of this policy, and awareness that the district uses monitoring systems to monitor and detect inappropriate use and tracking systems to track and recover lost or stolen equipment.

Student user agreements shall also be signed by a parent/guardian.

The Superintendent 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 users, approve activities, provide leadership for proper training for all users in the use of the CIS systems and the requirements of this policy, establish a system to ensure adequate supervision of the CIS systems, maintain executed user acknowledgement/consent forms, and interpret and enforce this policy.

The Superintendent or designee will establish a process for setting up individual and class accounts, set quotas for disk usage on the system, establish records management policies and records retention schedules to include electronically stored information, and establish the district's virus protection process.[21]

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 district, and to abide by the rules established by the district, its ISP, and local, state and federal laws.

The Superintendent or designee shall be responsible for recommending technology and developing procedures used to determine whether the district's computers are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedures shall include but not be limited to:[2][3][22]

1. Utilizing a technology protection measure that blocks or filters Internet access for minors and adults to certain visual depictions that are obscene, child pornography, harmful to minors with respect to use by minors, or determined inappropriate for use by minors by the Board.

2. Maintaining and securing a usage log.

3. Monitoring online activities of minors.

The Superintendent or designee shall develop and implement administrative regulations that ensure students are educated on network etiquette and other appropriate online behavior,

including interacting with other individuals on social networking web sites and in chat rooms and cyberbullying awareness and response.[3][12][23]

Guidelines

Computers, network, Internet, electronic communications, information systems, databases, files, software, and media, collectively called CIS systems, provide vast, diverse and unique resources. The Board will provide access to the district's CIS systems for users if there is a specific 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 district.

For users, the district's CIS systems must be used for education-related purposes and performance of district job duties in compliance with this policy. For employees, incidental personal use of district computers is permitted as defined in this policy, but they should have no expectation of privacy in anything they create, store, send, receive, or display on or over the district's CIS systems, including their personal files. Students may only use the CIS systems for educational purposes.

Users must practice proper etiquette and district ethics, must agree to the requirements of this policy, and are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

1. Be polite and do not become abrasive in messages to others. General district rules, regulations and policies for behavior and communicating apply.[15][17]

2. Use appropriate language and 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 email is not private or confidential.

5. Do not use the Internet or email in any way that would interfere with or disrupt its use by other users.

6. Consider all communications and information accessible via the district's Internet provider to be the property of the district.

7. Do not order any personal materials or use personal credit cards while using the district's computers.

8. Respect the rights of other users to an open and hospitable technology environment, regardless of race, sexual orientation, color, religion, national origin, gender, creed, ethnicity, age, marital status, political beliefs, or disability status.

Access to the CIS Systems

Users' CIS systems accounts 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 district authorities.

This policy, as well as other relevant Board policies, rules and administrative regulations, will govern use of the district's CIS systems for users.

Types of services that could be accessed through the district's CIS systems include, but are not limited to:

1. World Wide Web - District employees, students, and guests will have access to the World Wide Web through the district's CIS systems, as needed.

2. Email - District employees may be assigned individual email accounts for work-related use, as needed. Students may be assigned individual email accounts, as necessary, by the Superintendent or designee at the recommendation of the teacher, who will also supervise the student's use of the email service.

3. Guest Accounts - Guests may receive an individual web account with the approval of the Superintendent 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 and comply with this policy and all other Board policies, procedures, regulations and rules, as well as ISP terms, local, state and federal laws, and may not damage the district's CIS systems. An applicable acknowledgment/consent form must be signed in writing or electronically by a guest, and if the guest is a minor a parent's/guardian's written or electronic signature is required.

4. Blogs - Employees may be permitted to have 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 and other applicable Board policies, administrative regulations and rules of the district.

5. Web 2.0 Second Generation And Web 3.0 Third Generation Web-Based Services - Certain 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 district; however, such use must be approved by the Superintendent or designee followed by training authorized by the district. Users must comply with this policy as well as any other relevant Board policy, rules or administrative regulations (including the copyright, participatory learning/collaborative/social networking regulations, and rules during such use).

Parental Notification and Responsibility

The district will notify the parents/guardians about the district's CIS systems and the policies governing their use. This policy contains restrictions on accessing inappropriate matter. There is a wide range of material available on the Internet, some of which may not be fitting with the particular values of the families of the students. It is not practically possible for the district to monitor and enforce wide range of social values in student use of the Internet. Further, the district recognizes that parents/guardians bear primary responsibility for transmitting their particular set of family values to their children. The district will encourage parents/guardians to specify to their children what material is and is not acceptable for their children to access through the district's CIS system.

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 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 district will not be responsible for material that is retrieved through the Internet, or the consequences that may result from them. The district will not be responsible for any unauthorized financial obligations, charges or fees resulting from access to the district's CIS systems. In no event will the 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 district's CIS systems for illegal, inappropriate, unacceptable, or unethical purposes by users is prohibited. The district reserves the right to determine if activity constitutes an acceptable or unacceptable use of the CIS systems.

The prohibitions listed in this policy are in effect any time district resources are accessed whether on district property, at district events, connected to the district's network, when using mobile commuting equipment, telecommunication facilities in unprotected areas or environments, directly from home, or indirectly through another ISP, and if relevant, when an employee or student uses their own equipment. Students must also comply with Board Policy 237 and accompanying pertinent administrativeregulations.[20]

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. Send, receive, view, upload, download, store, access, print, distribute, or transmit material that is harmful to minors, indecent, obscene, pornographic, child pornographic, terroristic, including but not limited to visual depictions. Examples include, taking, disseminating, transferring, or sharing obscene, pornographic, lewd, or otherwise illegal images or photographs, whether by electronic data transfer or otherwise (such as, sexting, e-mailing, texting, among others). Neither may users advocate the destruction of property.

3. Send, receive, view, upload, download, store, access, print, distribute, or transmit inappropriate matter and material likely to be offensive or objectionable to recipients.

4. Bullying/Cyberbullying another individual.[12][23]

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, profane, 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. Students must obtain consent from their teacher to use IRC's; however, they may not use instant messaging or text messaging. Employees may only use instant messaging if consent was obtained from the Superintendent or designee.

9. Facilitate any illegal activity.

10. Communicate through email for noneducational purposes or activities, unless it is for incidental personal use as defined in this policy. The use of email to mass mail noneducational or nonwork related information is expressly prohibited (for example, the use of the everyone distribution list, building level distribution lists, or other email distribution 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 Board policies); conduct unauthorized fundraising or advertising on behalf of the district and nonschool organizations; resale 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. School district acquisition policies must be followed for district purchase of goods or supplies through the district system.[24][25][26][27][28]

12. Engage in political lobbying.

13. Install, distribute, reproduce or use unauthorized copyrighted software on district computers, or copy district software to unauthorized computer systems, intentionally infringing upon the intellectual property rights of others or violating a copyright.[29]

14. Install computer hardware, peripheral devices, network hardware or system hardware. The authority to install hardware or devices on district computers is restricted to the Superintendent or designee.

15. Encrypt messages using encryption software that is not authorized by the district from any access point on district equipment or district property. Users must use district approved encryption to protect the confidentiality of sensitive or critical information in the district's approved manner.

16. Access, interfere, possess, or distribute confidential or private information without permission of the district's administration. An example includes accessing other students' accounts to obtain their grades, or accessing other employees' accounts to obtain information.

17. Violate the privacy or security of electronic information.

18. 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.

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

20. Post personal or professional web pages without administrative approval.

21. Post anonymous messages.

22. Use the name of the Pleasant Valley School District in any form in blogs, on district Internet pages or web sites not owned or related to the district, or in forums/discussion boards, and social networking web sites, to express or imply the position of the district without the expressed, written permission of the Superintendent or designee. When such permission is granted, the posting must state that the statement does not represent the position of the district.

23. Bypass or attempt to bypass Internet filtering software by any method including, but not limited to, the use of anonymizer/proxies or any web sites that mask the content the user is accessing or attempting to access.

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

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

26. Use location devices to harm another person.

Access and Security Prohibitions -

Users must immediately notify the Superintendent or designee if they have identified a possible security problem. Users must read, understand, and submit an electronically or written signed acknowledgement form(s), and comply with this policy that includes network, Internet usage, electronic communications, telecommunications, nondisclosure, and physical and information security requirements. 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. Users are required to use unique strong passwords that comply with the district's password, authentication and syntax requirements. Users must not acquire or attempt to acquire User ID and 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 whether 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 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 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.

8. Accessing any website that the district has filtered or blocked as unauthorized. Examples include, but are not limited to, unauthorized social networking, music download, and gaming sites.

9. Users must protect and secure all electronic resources and information data and records of the district from theft and inadvertent disclosure to unauthorized individuals or entities when they are under the supervision and control of the district and when they are not under supervision and control of the district, for example, but not limited to, working at home, on vacation or elsewhere. If any user becomes aware of the release of district information, data or records, the release must be reported to the Superintendent or designee immediately.[30]

Operational Prohibitions -

The following operational activities and behaviors are prohibited:

1. Interference with, infiltration into, or disruption of the CIS systems, network accounts, services or equipment of others, including, but not limited to, the propagation of computer "worms" and "viruses", Trojan Horse, trapdoor, robot, spider, crawler, and other program code, the sending of electronic chain mail, 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 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.

4. Attempting to alter any district computing or networking components (including, but not limited to fileservers, 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 retransmission of any computer, electronic communications systems, or network services, whether wired, wireless, cable, virtual, cloud, 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 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, networking equipment through the users' negligence or deliberate act, including, but not limited to vandalism.

12. Failing to comply with requests from district staff 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 student's date of birth, Social Security number, driver's license number, financial information, credit card number, health information, phone numbers, 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.

4. Documents, web pages and electronic communications must conform to all district policies and guidelines.

5. Documents to be published on the Internet must be edited and approved according to district procedures before publication.

Copyright Infringement and Plagiarism

Federal laws and regulations pertaining to copyright will govern the use of material accessed through district resources. Users will make a standard practice of requesting permission from the holder of the work, complying with the fair use doctrine, and/or complying with license agreements. Employees will instruct users to respect copyrights.[29][31]

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.

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.

District guidelines on plagiarism will govern use of material accessed through the 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 district's CIS systems may involve the district's use of plagiarism analysis software being applied to their work.

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 must select material that is appropriate in light of the age of the students and that is relevant to the course objectives. Teachers must preview the materials and web sites they require or recommend students access to determine the appropriateness of the material contained on or accessed through the web site. Teachers must provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly. Teachers must assist their students in developing the critical thinking skills necessary to ascertain the truthfulness of information, distinguish fact from opinion, and engage in discussions about controversial issues while demonstrating tolerance and respect for those who hold divergent views.

District Website

The district has established and maintains a website and will develop and modify its web pages that will present information about the district under the direction of the Superintendent or designee. Publishers must comply with this policy and other pertinent Board policies.[32]

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 district personal and private information/data, images and copyrighted material in their blog, and may not disrupt the district.

Conduct otherwise will result in actions further described in this policy and provided in other relevant Board policies.

Safety and Privacy

It is the district's goal to protect users of the district's CIS systems from harassment and unwanted or unsolicited electronic communications. Any user who receives threatening or unwelcome electronic communications or inadvertently visits or accesses an inappropriate site shall report such immediately to the Superintendent or designee. Network users shall not reveal personal information to other users on the network, including chat rooms, email, social networking websites, etc.[3]

Internet safety measures shall effectively address the following:[3][22]

1. Control of access by minors to inappropriate matter on the Internet and World Wide Web.

2. Safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications.

3. Prevention of unauthorized online access by minors, including "hacking" and other unlawful activities.

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

5. Restriction of minors' access to materials harmful to them.

If the district requires that data and information be encrypted, users must use district authorized encryption to protect their security.

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, 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 for employees), dismissal, expulsions, and/or legal proceedings on a case-by-case basis. This policy incorporates all other relevant Board policies and district rules such as, but not limited to, the student and professional employee discipline policies, applicable Code of Student Conduct, copyright, property, curriculum, terroristic threat, vendor access, and harassment policies.[10][11][15][16][17][29][33]

Users are responsible for damages to the network, equipment, electronic communications systems, and software resulting from negligent, deliberate, and willful acts. Users will also be responsible for incidental or unintended damage resulting from willful or deliberate violations of this policy.[14]

Violations as described in this policy may be reported to the district, 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 and/or criminal prosecution. 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.

Any and all costs incurred by the district for repairs and/or replacement of software, hardware and data files and for technological consultant services due to any violation of this policy, or federal, state, or local law, shall be paid by the user who caused the loss.

No. 815-AR

PLEASANT VALLEY
SCHOOL DISTRICT

ADMINISTRATIVE
REGULATION

815-AR. ADMINISTRATIVE REGULATIONS FOR THE USE OF THE SCHOOL DISTRICT E-MAIL SYSTEM

The Board recognizes the need for staff to use school district electronic mail (e-mail) as a means of communication and asserts that such use shall be for legitimate educational purposes only. All e-mail use must conform to the school district's acceptable use policy (Board Policy No. 815). E-mail is not guaranteed to be private and confidential and may be read by authorized school district personnel. E-mail users are reminded that e-mails may be forwarded to other parties. The following e-mail guidelines are intended to assist the staff member in the proper use of school district e-mail. Additionally, school staff is reminded that a large percentage of our students are already using e-mail at home. We, as adults in the educational community, have a responsibility to teach them e-mail etiquette. Following the guidelines below will help us to model effective and responsible e-mail communication.

A. Etiquette

1. Clarity
   This is probably the most important consideration when you send an e-mail message. Here are some points to keep in mind: Be brief but clear. Long messages often go unread. Say only what is necessary. Don't forget writing conventions of grammar, punctuation and spelling. While it may be okay for students to be less formal when they instant message their friends it is not okay for general audiences. Avoid abbreviations unless you are sure your reader knows what they mean. If you're not sure that your reader knows that BTW means "by the way," spell it out.

2. Shouting
   On the Internet the use of all caps is perceived as shouting (as well as being very difficult to read). Use other formatting or language for emphasis but avoid expressing emotion unless it is a positive experience.

3. Privacy
   One of the most important things to remember is that nothing online is private. Because e-mail is so quick and easy it also seems transitory but it is surprisingly permanent, and once you send it, you have no control over who sees it. A good rule is never write anything in an e-mail that you wouldn't want to see on the front page of your local newspaper. Be very careful about including confidential student information in an e-mail. Sometimes it's better just to pick up the phone.

4. Signature
Not everyone knows who you are from your e-mail address alone. The easiest way to make sure everyone knows who you are is to create a signature file. A signature should contain **only** your name, position, school, your school's phone number, your extension and our web address.

5. Attachments
Be careful about sending large attachments. They can take a long time to download and some recipients may use mail systems that restrict attachments. If you are sending an attachment, let the recipient know in the body of your message what the attachment is and why you are sending it. Attachments are notorious for spreading viruses and it's wise not to open one unless you know what it is and who sent it.

6. Subject Line
The subject line is important; please don't leave it blank. It is also important that your subject line is meaningful. People who receive hundreds of e-mails a day scan those subject lines before deciding which e-mails to read and respond to. A meaningful subject line also helps when you are organizing your messages or trying to search for and retrieve an old message.

7. "Cc"-ing
If you decide to "Cc" your message to someone, please state in the message why you are doing so, especially if the "Cc" recipient is not expecting the message. Be clear about who is expected to act on the message and who is receiving it just for information. Limit "Cc"-ing to only those important to the situation at hand. When you cc to the world it can be seen as ganging up or a bullying tactic and it is generally unnecessary.

8. Replying
It is important that you reply to your messages as quickly as possible. This may be difficult if you receive a lot of mail but it's polite to at least acknowledge that you received it. You can send a quick, one-line reply saying that you received the message and will send a longer reply later. If the message has been sent to several people, it may be appropriate to reply only to the sender. On the other hand, your reply may contain information that everyone needs to have. You should also be thoughtful about how much of the original message you quote. E-mail accounts should be checked, at best, twice daily, in the morning and afternoon at minimum.

9. Forwarding
If you decide to forward a message to someone else, let the sender know so he or she will expect a reply from that person and not be confused by it. It's also a good idea to let the person you are forwarding the message to know why you are forwarding it. Do not forward jokes or other junk mail.

B. Staff-to-Student Electronic Messaging

Users should not assume that electronic communications are private or confidential. When completing the "To:" field, it is especially important that users are careful to send messages only to the intended recipient(s).

1. E-mails, texts, or any other form of electronic messaging generated by faculty and/or staff to students shall only be directed to entire school-sponsored student groups, clubs or teams and shall only involve issues specifically related to classroom work or sport/activity related information.

2. Faculty and staff may respond to individual students via e-mail when it involves issues specifically related to classroom work or sport/activity related information.

3. Electronic messaging by faculty or staff to students shall be solely for the purpose of informing students of time sensitive information (e.g., canceled practices, reminders, rescheduling, classroom-specific assignments).

4. All e-mail messaging to students shall only be done through the staff member's *pvbears.org* Outlook account.

5. All electronic communications shall include a "Cc" to the appropriate building principal and, as is applicable, the Athletic/Activities Director.

6. Please see No. 815-AR-1 for guidelines regarding safe and responsible blogging.

No. 817-AR

PLEASANT VALLEY
SCHOOL DISTRICT

ADMINISTRATIVE
REGULATION

817-AR. SEXTING

Sexting can be defined as the act of text messaging someone in the hopes of having a sexual encounter with them at a future time. It may be initially casual, but may transition into something highly suggestive and/or sexually explicit. It has also been defined as the practice of sending or posting sexually suggestive text messages and images, including semi-nude or nude photographs via cell phones or over the internet.

At no time should a staff member knowingly view or attempt to access any material in question.

Any staff member who receives a sexually explicit electronic message through their phone or on their computer from either a student, parent/guardian, another staff member or someone else should immediately contact their building administrator or immediate supervisor.

Once an administrator has learned that there has been a case that could involve sexting, he/she must proceed expeditiously, but with great caution. If the administrator receives information that a cell phone or computer contains a nude depiction, the picture is not to be opened and viewed. Instead, the cell phone, laptop, external hard drive zip drive or other electronic device is to be placed in a sealed envelope and immediately turned over to the police for their inspection and evaluation. For a desktop computer, the item is to be boxed and sealed. In addition, the following language is to be affixed to the sealed envelope or box.

EVIDENCE

NOTICE:

This envelope contains evidence that might contain unlawful images. No conclusions are being made by the school district or any of its employees or officials as to whether any of the depictions are unlawful. However, since there is the possibility that one or more images may be unlawful, the contents remain under seal to be turned over to the police.

This disclaimer helps to eliminate the potential risk for a defamation suit and drives home the point that administrators must be very careful before accusing anyone of engaging in an unlawful act.

Determining the unlawfulness of any possible act of sexting is a job for law enforcement. Administrators are not to leap to the conclusion that a suspected incident of sexting has resulted in an unlawful act. Consultation with the school district's solicitor is thus warranted.

Administrators who encounter possible incidents of sexting are to immediately contact the Superintendent and/or designee.

PLEASANT VALLEY
SCHOOL DISTRICT

ADMINISTRATIVE
REGULATION

NO. 817-AR-1 USE OF PERSONAL COMPUTERS/ELECTRONIC DEVICES IN THE SCHOOL SETTING

I. Employees Performing School District Work/Business

A. Employees are prohibited from using their own computer/electronic device for school district purposes.

B. Employees are prohibited from using or saving school district work on hard drives, servers, clouds (such as Google docs and other "cloud" resources) or removal devices (such as portable hard-drives or thumb-drives) that are not subject to the control and ready access of the school district.

II. Registration of Computers/Electronic Devices

Any computer/electronic device that will be brought to and accessed at school or at a school-sponsored activity or function must be properly be registered with the school district.

III. Privacy and Searches

The school district does not allow students to bring their own computers/electronic devices to school unless the student and his/her parent/guardian consent in writing to searches of their computers/electronic devices.

IV. Repairs

School district personnel are not authorized to repair a student-owned device.

V. Student and Employee Rules

A. Computers/electronic devices brought to school and used on the school district's network must be approved by the principal or Technology Systems Coordinator and/or their designee(s) prior to such use;

B. Students and employees cannot access their computers/electronic devices without a password and username;

C. The school district's network cannot be accessed without the password and username; and

D. Students and employees must not divulge their passwords and usernames to others.

VI. Tracking Computer Activity

The school district's technology department has the ability and is within its authority to track and report all activity on individual computers/electronic devices, including those brought to school when they are on the school district's network.

VII. Blocking and Filtering

The school district's technology department is within its authority to install blocking and filtering software as required by law.

VIII. Bring Your Own Device (BYOD) – Students.

In recognition of the significance of computers/electronic devices in today's society, work and school, and the fact that many students have their own computers/electronic devices that can be used for proper educational purposes, the school district may allow students to bring their own computers/electronic devices to school and to use said computers/electronic devices subject to the following rules or instructions as may be imposed by the school district staff and providing such use has an identified legitimate educational purpose:

A. Students shall be solely responsible for the safekeeping of any computer/electronic device brought to school and each student who brings a computer/electronic device to school or to a school function or activity shall assume the risk of loss, theft, damage or other injury to the computer/electronic device.

B. Prior to bringing any computer/electronic device to school or to a school-sponsored activity, students shall register the computer/electronic device with the principal or designee of the school to which the student is assigned by completing a form used by the school district for such purpose. No student shall bring any computer/electronic device to school or to a school-sponsored function or activity that is not registered. The school district has a right to confiscate any computer/electronic device that is brought to school and that has not been properly registered by the student and his/her parent/guardian.

C. All rules and prohibitions stated in this policy that are applicable to students shall apply as applicable to the use of a student's computer/electronic device that is brought to school.

D. Students shall not use the audio recording function of any computer/electronic device at school or at any school-sponsored activity or function unless given express and specific permission in advance by: (1) the school principal or designee; and (2) the individuals whose voices or activities are being recorded.

E. Students shall not use the camera or video recording function of any computer/electronic device at school or at any school-sponsored activity or function unless given express and specific permission in advance by: (1) the school principal or designee; and (2) the individuals who are being recorded.

F. The school district has the right to confiscate any computer/electronic device that is brought to school or to a school-sponsored function or activity: (1) that has not been approved in accordance with policy and/or regulation; (2) that is used in violation of any of the rules or prohibitions contained in policy and/or regulation; or (3) that is used or "out" or "on" in violation of any instructions or directives by any teacher, administrator or other person who is in charge of the function or activity.

G. Confiscated computers/electronic devices. Any computer/electronic device that is confiscated in accordance with these regulations shall be returned only to the student's parent/guardian and on such terms and conditions as shall be determined by the school district. As a disciplinary consequence, the school district may keep the computer/electronic device for the balance of the school year. This disciplinary response is in addition to any other disciplinary response that may be appropriate under the circumstances.

H. Under no circumstances shall the school district be responsible at any time for any fees or charges that may be associated with a computer/electronic device brought to school by a student, including the cost of the computer/electronic device, monthly fees or charges, access fees, Internet access fees or any other similar fee. All such fees, costs and charges remain the sole responsibility of the student and/or his/her parent(s)/guardian(s).

X. BYOD – Employees.

A. Employees may bring their own computers/electronic devices to school subject to the following rules and such rules or instructions as may be imposed by their supervisor.

B. Employees shall be solely responsible for the safekeeping of any computer/electronic device brought to school and each employee who brings a computer/electronic device to school or to a school-sponsored function or activity shall assume the risk of loss, theft, damage or other injury to the electronic device.

C. No school district, employee or student data or information may be used in any fashion on any computer/electronic device that is not owned by the school district.

D. Prior to bringing any computer/electronic device to school or to a school-sponsored activity or function, employees shall register the computer/electronic device with their supervisor and/or the principal or designee of the school to which the employee is assigned by completing a form used by the school district for such purpose. No employee shall bring any computer/electronic device to school that is not registered. The school district has the right to confiscate any computer/electronic device that is brought to school and has not been properly approved.

E. All rules and prohibitions stated in these regulations that are applicable to employees shall apply as applicable to the use of an employee's computer/electronic device that is brought to school.

F. Employees shall not use the audio recording function of any computer/electronic device at school or at any school-sponsored activity or function unless given express and specific permission in advance by: (1) their supervisor and/or the principal or designee of the school to which the employee is assigned; and (2) the individuals whose voices or activities are being recorded.

G. Employees shall not use the camera or video recording function of any computer/electronic device at school or at any school-sponsored activity or function unless given express and specific permission in advance by: (1) the supervisor and/or the principal or designee of the school to which the employee is assigned; and (2) the individuals who are being recorded.

H. The school district has the right to confiscate any computer/electronic device that is brought to school or to a school-sponsored function or activity: (1) that is not properly registered in accordance with these regulations; or (2) that is used in violation of any of the rules or prohibitions contained herein.

I. Under no circumstances shall the school district be responsible at any time for any fees or charges that may be associated with a computer/electronic device brought to school or a school-sponsored event or function by an employee, including the cost of the computer or electronic device, monthly fees or charges, access fees, telephone service charges, data fees, Internet access fees or any other similar fee. All such fees, costs and charges remain the sole responsibility of the employee(s).

XI. Privacy provisions pertaining to BYOD:

A. No employee or student using the school district's digital technology shall have any right of privacy or expectation of privacy with respect to anything done with said digital technology. The digital technology belongs to, is licensed to, or accessible through digital technology that is owned by or licensed to the school district. The school district retains all right as an owner or licensee with respect to all digital technology that it owns or licenses and has, unless restricted by an express agreement with a third-party supplier, the rights of an owner or licensee, including, the rights to use, transfer, inspect, look in, read, store or store any such digital technology.

B. The school district reserves the right to review emails to or from students, parents/guardians or employees to ensure that this policy is being complied with.

C. Notwithstanding anything herein to the contrary, no employee shall read or examine emails of members of the Board of School Directors (School Board) except: (1) when necessary to comply with or respond to a public records request, a litigation hold requirement, or an order or subpoena in connection with an administrative or judicial action; or (2) after written notice has been provided to the School Board member that his or her email will be reviewed.

D. The school district shall have the right to send communications of any kind that is sent to a school district maintained account, including, but not limited to, emails, text

messages or tweets, to other recipients when deemed in the interests of the school district to do so, including, to ensure quality control, to ensure compliance with these regulations, and/or when an employee or official is on leave or suspension or has been discharged, resigned, retired or otherwise separated from employment. The sending of such communications may be done manually, automatically, or through any other means or methods chosen by the school district and employees and students shall be deemed to have consented to these procedures by their use of the school district's systems.

E. The school district shall have the right to insert messages into electronic communications, including emails, instant messages and tweets, that may appear to be coming from the employee or student.

Book	Policy Manual
Section	800 Operations
Title	Maintaining Professional Adult/Student Boundaries
Number	824
Status	Active
Legal	1. 24 P.S. 510 2. Pol. 818 3. Pol. 103 4. Pol. 103.1 5. Pol. 248 6. Pol. 815 7. 23 Pa. C.S.A. 6311 8. Pol. 806 9. 24 P.S. 2070.9a 10. Pol. 317.1 11. 24 P.S. 1302.1-A 12. 24 P.S. 1303-A 13. 22 PA Code 10.2 14. 22 PA Code 10.21 15. 22 PA Code 10.22 16. Pol. 805.1 17. Pol. 348 18. Pol. 317 22 PA Code 235.1 et seq 24 P.S. 2070.1a et seq 23 Pa. C.S.A. 6301 et seq
Adopted	May 25, 2017

Authority

This policy applies to district employees, volunteers, student teachers, and independent contractors and their employees who interact with students or are present on school grounds. For purposes of this policy, such individuals are referred to collectively as **adults**. The term **adults** as used in this policy, does not include district students who perform services on a volunteer or compensated basis.

All adults shall be expected to maintain professional, moral and ethical relationships with district students that are conducive to an effective, safe learning environment. This policy

addresses a range of behaviors that include not only obviously unlawful or improper interactions with students, but also precursor grooming and other boundary-blurring behaviors that can lead to more egregious misconduct.

The Board directs that all adults shall be informed of conduct that is prohibited and the disciplinary actions that may be applied for violation of Board policies, administrative regulations, rules and procedures.[1]

This policy is not intended to interfere with appropriate pre-existing personal relationships between adults and students and their families that exist independently of the district or to interfere with participation in civic, religious or other outside organizations that include district students.

Definition

For purposes of this policy, **legitimate educational reasons** include matters or communications related to teaching, counseling, athletics, extracurricular activities, treatment of a student's physical injury or other medical needs, school administration or other purposes within the scope of the adult's job duties.

Delegation of Responsibility

The Superintendent or designee shall annually inform students, parents/guardians, and all adults regarding the contents of this Board policy through employee and student handbooks, posting on the district website, and by other appropriate methods.

The building principal or designee shall be available to answer questions about behaviors or activities that may violate professional boundaries as defined in this policy.

Independent contractors doing business with the district shall ensure that their employees who have interaction with students or are present on school grounds are informed of the provisions of this policy.[2]

Guidelines

Adults shall establish and maintain appropriate personal boundaries with students and not engage in any behavior that is prohibited by this policy or that creates the appearance of prohibited behavior.

Prohibited Conduct

Romantic or Sexual Relationships -

Adults shall be prohibited from dating, courting, or entering into or attempting to form a romantic or sexual relationship with any student enrolled in the district, regardless of the student's age. Students of any age are not legally capable of consenting to romantic or sexual interactions with adults.

Prohibited romantic or sexual interaction involving students includes, but is not limited to:

1. Sexual physical contact.
2. Romantic flirtation, propositions, or sexual remarks.
3. Sexual slurs, leering, epithets, sexual or derogatory comments.

4. Personal comments about a student's body.
5. Sexual jokes, notes, stories, drawings, gestures or pictures.
6. Spreading sexual or romantic rumors.
7. Touching a student's body or clothes in a sexual or intimate way.
8. Accepting massages, or offering or giving massages other than in the course of injury care administered by an athletic trainer, coach, or health care provider.
9. Restricting a student's freedom of movement in a sexually intimidating or provocative manner.
10. Displaying or transmitting sexual objects, pictures, or depictions.

Social Interactions -

In order to maintain professional boundaries, adults shall ensure that their interactions with students are appropriate.

Examples of prohibited conduct that violates professional boundaries include, but are not limited to:

1. Disclosing personal, sexual, family, employment concerns or other private matters to one or more students.
2. Exchanging notes, emails or other communications of a personal nature with a student.
3. Giving personal gifts, cards or letters to a student without written approval from the building principal.
4. Touching students without a legitimate educational reason. (Reasons could include the need for assistance when injured, a kindergartner having a toileting accident and requiring assistance, appropriate coaching instruction, or appropriate music instruction).
5. Singling out a particular student or students for personal attention or friendship beyond the ordinary professional adult-student relationship.
6. Taking a student out of class without a legitimate educational reason.
7. Being alone with a student behind closed doors without a legitimate educational reason.
8. Initiating or extending contact with a student beyond the school day or outside of class times without a legitimate educational reason.
9. Sending or accompanying a student on personal errands.
10. Inviting a student to the adult's home.
11. Going to a student's home without a legitimate educational reason.
12. Taking a student on outings without prior notification to and approval from both the parent/guardian and the building principal.

13. Giving a student a ride alone in a vehicle in a nonemergency situation without prior notification to and approval from both the parent/guardian and the building principal.

14. Addressing students or permitting students to address adults with personalized terms of endearment, pet names, or otherwise in an overly familiar manner.

15. Telling a student personal secrets or sharing personal secrets with a student.

16. For adults who are not guidance/counseling staff, psychologists, social workers or other adults with designated responsibilities to counsel students, encouraging students to confide their personal or family problems and/or relationships. If a student initiates such discussions, the student should be referred to the appropriate school resource.

17. Furnishing alcohol, drugs or tobacco to a student or being present where any student is consuming these substances.

18. Engaging in harassing or discriminatory conduct prohibited by other district policies or by state or federal law and regulations.[3][4][5]

Electronic Communications -

For purposes of this policy, **electronic communication** shall mean a communication transmitted by means of an electronic device including, but not limited to, a telephone, cellular telephone, computer, computer network, personal data assistant or pager. Electronic communications include, but are not limited to, emails, instant messages and communications made by means of an Internet website, including social media and other networking websites.

As with other forms of communication, when communicating electronically, adults shall maintain professional boundaries with students.

Electronic communication with students shall be for legitimate educational reasons only.

When available, district-provided email or other district-provided communication devices shall be used when communicating electronically with students. The use of district-provided email or other district-provided communication devices shall be in accordance with district policies and procedures.[6]

All electronic communications from coaches and advisors to team or club members shall be sent in a single communication to all participating team or club members, except for communications concerning an individual student's medical or academic privacy matters, in which case the communications will be copied to the building principal. In the case of sports teams under the direction of the Athletic Director, such medical or academic communications shall also be copied to the Athletic Director.

Adults shall not follow or accept requests for current students to be friends or connections on personal social networking sites and shall not create any networking site for communication with students other than those provided by the district for this purpose, without the prior written approval of the building principal.

Exceptions

An emergency situation or a legitimate educational reason may justify deviation from professional boundaries set out in this policy. The adult shall be prepared to articulate the reason for any deviation from the requirements of this policy and must demonstrate that s/he has maintained an appropriate relationship with the student.

Under no circumstance will an educational or other reason justify deviation from the "Romantic and Sexual Relationships" section of this policy.

There will be circumstances where personal relationships develop between an adult and a student's family, e.g. when their children become friends. This policy is not intended to interfere with such relationships or to limit activities that are normally consistent with such relationships. Adults are strongly encouraged to maintain professional boundaries appropriate to the nature of the activity.

It is understood that many adults are involved in various other roles in the community through nondistrict-related civic, religious, athletic, scouting or other organizations and programs whose participants may include district students. Such community involvement is commendable, and this policy is not intended to interfere with or restrict an adult's ability to serve in those roles; however, adults are strongly encouraged to maintain professional boundaries appropriate to the nature of the activity with regard to all youth with whom they interact in the course of their community involvement.

Reporting Inappropriate or Suspicious Conduct

Any person, including a student, who has concerns about or is uncomfortable with a relationship or interaction between an adult and a student, shall immediately notify the Superintendent, principal or other administrator.[5]

All district employees, independent contractors and volunteers who have reasonable cause to suspect that a child is the victim of child abuse, shall immediately report the suspected abuse, in accordance with applicable law, regulations and Board policy.[7][8]

An educator who knows of any action, inaction or conduct which constitutes sexual abuse or exploitation or sexual misconduct under the Educator Discipline Act shall report such misconduct to the Pennsylvania Department of Education on the required form, and shall report such misconduct to the Superintendent and his/her immediate supervisor, within fifteen (15) days of discovery of such misconduct.[9][10]

If the Superintendent or designee reasonably suspects that conduct being reported involves an incident required to be reported under the Child Protective Services Law, the Educator Discipline Act or the Safe Schools Act, the Superintendent or designee shall make a report, in accordance with applicable law, regulations and Board policy.[7][9][11][12][13][14][15][10][16][8]

It is a violation of this policy to retaliate against any person for reporting any action pursuant to this policy or for participating as a witness in any related investigation or hearing.

Investigation

Allegations of inappropriate conduct shall be promptly investigated in accordance with the procedures utilized for complaints of harassment.[5][17]

It is understood that some reports made pursuant to this policy will be based on rumors or misunderstandings; the mere fact that the reported adult is cleared of any wrongdoing shall not result in disciplinary action against the reporter or any witnesses. If as the result of an investigation any individual, including the reported adult, the reporter, or a witness is found to have intentionally provided false information in making the report or during the investigation or hearings related to the report, or if any individual intentionally obstructs the investigation or hearings, this may be addressed as a violation of this policy and other applicable laws, regulations and district policies. **Obstruction** includes, but is not limited to, violation of "no

contact" orders given to the reported adult, attempting to alter or influence witness testimony, and destruction of or hiding evidence.

Disciplinary Action

A district employee who violates this policy may be subject to disciplinary action, up to and including termination, in accordance with all applicable district disciplinary policies and procedures.[18]

A volunteer, student teacher, or independent contractor or an employee of an independent contractor who violates this policy may be prohibited from working or serving in district schools for an appropriate period of time or permanently, as determined by the Superintendent or designee.

Training

The district shall provide training with respect to the provisions of this policy to current and new district employees, volunteers and student teachers subject to this policy.

The district, at its sole discretion, may require independent contractors and their employees who interact with students or are present on school grounds to receive training on this policy and related procedures.