Policy - Subcommittee Meeting

Thursday, October 15, 2026 5:45 PM
Main Office Conference Room #205 , 3115 Ridge Road, Perkasie, PA 18944

1. **Call to Order**

2. **Committee Review**

2.A. 806 - Child Abuse Policy

BOARD POLICY

806 Child Abuse

POLICY NUMBER	ADOPTED	VERSION	DOCUMENT STATUS
806	3/19/2026	v1	ACTIVE

PRINTED
10/9/2026

Authority

The Joint Operating Committee requires school employees, independent contractors, and volunteers to comply with identification and reporting requirements for suspected child abuse, as well as the training requirement for recognition and reporting of child abuse in order to comply with the Child Protective Services Law and the School Code.[1][2] **[3]** **[4]**

Definitions

The following words and phrases, when used in this policy, shall have the meaning given to them in this section:

Adult - an individual eighteen (18) years of age or older.[5]

Bodily injury - impairment of physical condition or substantial pain.[5]

Certifications - refers to the child abuse history clearance statement and state and federal criminal history background checks required by the Child Protective Services Law and/or the School Code.[6] [7]

Child - an individual under eighteen (18) years of age.[5]

Child abuse - intentionally, knowingly, or recklessly doing any of the following:[5]

1. Causing bodily injury to a child through any recent act or failure to act.

2. Fabricating, feigning, or intentionally exaggerating or inducing a medical symptom or disease which results in a potentially harmful medical evaluation or treatment to the child through any recent act.

3. Causing or substantially contributing to serious mental injury to a child through any act or failure to act or a series of such acts or failures to act.

4. Causing sexual abuse or exploitation of a child through any act or failure to act.

5. Creating a reasonable likelihood of bodily injury to a child through any recent act or failure to act.

6. Creating a likelihood of sexual abuse or exploitation of a child through any recent act or failure to act.

7. Causing serious physical neglect of a child.

8. Engaging in any of the following recent acts:

    a. Kicking, biting, throwing, burning, stabbing, or cutting a child in a manner that endangers the child.

    b. Unreasonably restraining or confining a child, based on consideration of the method, location, or the duration of the restraint or confinement.

    c. Forcefully shaking a child under one (1) year of age.

    d. Forcefully slapping or otherwise striking a child under one (1) year of age.

    e. Interfering with the breathing of a child.

    f. Causing a child to be present during the operation of a methamphetamine laboratory, provided that the violation is being investigated by law enforcement.[8]

    g. Leaving a child unsupervised with an individual, other than the child's parent, who the actor knows or reasonably should have known was required to register as a Tier II or Tier III sexual offender, has to register for life, or has been determined to be a sexually violent predator or sexually violent delinquent.[9][10][11][12]

9. Causing the death of the child through any act or failure to act.

10. Engaging a child in a severe form of trafficking in persons or sex trafficking, as those terms are defined in the law.[13]

The term **child abuse** does not include physical contact with a child that is involved in normal participation in physical education, athletic, extracurricular, or recreational activities. Also excluded from the meaning of the term **child abuse** is the use of reasonable force by a person responsible for the welfare of a child for purposes of supervision, control, or safety, provided that the use of force:[14]

1. Constitutes incidental, minor, or reasonable physical contact in order to maintain order and control;

2. Is necessary to quell a disturbance or remove a child from the scene of a disturbance that threatens property damage or injury to persons;

3. Is necessary for self-defense or defense of another;

4. Is necessary to prevent the child from self-inflicted physical harm; or

5. Is necessary to gain possession of weapons, controlled substances, or other dangerous objects that are on the person of the child or in the child's control.

Direct contact with children - the possibility of care, supervision, guidance, or control of children or routine interaction with children.[1]

Independent contractor - an individual other than a school employee who provides a program, activity, or service who is otherwise responsible for the care, supervision, guidance, or control of children pursuant to a contract. The term does not apply to administrative or other support personnel unless the administrative or other support personnel have direct contact with children.[5] [15]

Perpetrator - a person who has committed child abuse and is a parent/guardian of the child; a spouse or former spouse of the child's parent/guardian; a paramour or former paramour of the child's parent/guardian; an individual fourteen (14) years of age or older who is responsible for the child's welfare or who has direct contact with children as an employee of child-care services, a school or through a program activity or service; an individual fourteen (14) years of age or older who resides in the same home as the child; or an adult who does not reside in the same home as the child but is related within the third degree of consanguinity or affinity by birth or adoption to the

child; or an adult who engages a child in severe forms of trafficking in persons or sex trafficking, as those terms are defined in the law. Only the following may be considered a perpetrator solely based upon a failure to act: a parent/guardian of the child; a spouse or former spouse of the child's parent/guardian; a paramour or former paramour of the child's parent/guardian; an adult responsible for the child's welfare; or an adult who resides in the same home as the child.[5][13]

Person responsible for the child's welfare - a person who provides permanent or temporary care, supervision, mental health diagnosis or treatment, training, or control of a child in lieu of parental care, supervision, and control.[5]

Program, activity, or service - any of the following in which children participate and which is sponsored by a school or a public or private organization:[5]

1. A youth camp or program.
2. A recreational camp or program.
3. A sports or athletic program.
4. A community or social outreach program.
5. An enrichment or educational program.
6. A troop, club, or similar organization.

Recent act or failure to act - any act or failure to act committed within two (2) years of the date of the report to the Department of Human Services of the Commonwealth or county agency.[5]

Routine interaction - regular and repeated contact that is integral to a person's employment or volunteer responsibilities.[5]

School employee - an individual who is employed by a school or who provides a program, activity, or service sponsored by a school. The term does not apply to administrative or other support personnel unless the administrative or other support personnel have direct contact with children.[5]

Serious mental injury - a psychological condition, as diagnosed by a physician or licensed psychologist, including the refusal of appropriate treatment, that:[5]

1. Renders a child chronically and severely anxious, agitated, depressed, socially withdrawn, psychotic, or in reasonable fear that the child's life or safety is threatened; or

2. Seriously interferes with a child's ability to accomplish age-appropriate developmental and social tasks.

Serious physical neglect - any of the following when committed by a perpetrator that endangers a child's life or health, threatens a child's well-being, causes bodily injury or impairs a child's health, development or functioning:[5]

1. A repeated, prolonged, or egregious failure to supervise a child in a manner that is appropriate considering the child's developmental age and abilities.

2. The failure to provide a child with adequate essentials of life, including food, shelter, or medical care.

Sexual abuse or exploitation - any of the following:[5]

1. The employment, use, persuasion, inducement, enticement, or coercion of a child to engage in or assist another individual to engage in sexually explicit conduct, which includes, but is not limited to, the following:

    a. Looking at the sexual or other intimate parts of a child or another individual for the purpose of arousing or gratifying sexual desire in any individual.

    b. Participating in sexually explicit conversation either in person, by telephone, by computer, or by a computer-aided device for the purpose of sexual stimulation or gratification of any individual.

    c. Actual or simulated sexual activity or nudity for the purpose of sexual stimulation or gratification of any individual.

    d. Actual or simulated sexual activity for the purpose of producing a visual depiction, including photographing, videotaping, computer depicting, or filming.

    The conduct described above does not include consensual activities between a child who is fourteen (14) years of age or older and another person who is fourteen (14) years of age or older and whose age is within four (4) years of the child's age.

2. Any of the following offenses committed against a child: rape; statutory sexual assault; involuntary deviate sexual intercourse; sexual assault; institutional sexual assault; aggravated indecent assault; indecent assault; indecent exposure; incest; prostitution; sexual abuse; unlawful contact with a minor; or sexual exploitation.

Student - an individual enrolled in the school under eighteen (18) years of age.[5]

Volunteer - an unpaid adult individual, who, on the basis of the individual's role as an integral part of a regularly scheduled program, activity, or service, is a person responsible for the child's welfare or has direct contact with children.[15]

Delegation of Responsibility

The Executive Director or designee shall:

1. Require each candidate for employment to submit an official child abuse clearance statement and state and federal criminal history background checks (certifications) as required by law.[6] [7] **[16]** **[17]** **[18]**

2. Require each applicant for transfer or reassignment to submit the required certifications unless the applicant is applying for a transfer from one position as an employee to another position as an employee of this school and the applicant's official child abuse certifications are current.[19] [20] **[21]**

School employees and independent contractors shall obtain and submit new certifications every sixty (60) months.[20]

Certification requirements for volunteers are addressed separately in Joint Operating Committee Policy 916. **[22]**

The Executive Director or designee shall annually notify school staff, independent contractors, and volunteers of their responsibility for reporting child abuse in accordance with Joint Operating Committee policy and administrative regulations.

The Executive Director or designee shall ensure that the poster, developed by the PA Department of Education, displaying the statewide toll-free telephone numbers for reporting suspected child abuse, neglect, and school safety issues be posted in a high-traffic, public area of each school building. The designated area shall be readily accessible and widely used by students.[23]

The Executive Director or designee shall annually inform students, parents/guardians, independent contractors, volunteers, and staff regarding the contents of this Joint Operating Committee policy.

Guidelines

Aiding and Abetting Sexual Abuse

School employees, acting in an official capacity for this school, are prohibited from assisting another school employee, contractor, or agent in obtaining a new job if the school employee knows, or has probable cause to believe, that such school employee, contractor, or agent engaged in sexual misconduct regarding a minor or student. **[16]** **[17]** **[18]** **[21]** [24][25] **[26]** **[27]**

This prohibition applies only to assistance that extends beyond the performance of normal processing of personnel matters, including routine transmission of files or other information. This prohibition shall not apply if:[25]

1. The relevant information has been properly reported to law enforcement officials and any other authority required by federal, state, or local law, and the matter has been officially closed, or the prosecutor or law enforcement officials have notified school officials that there is insufficient information to establish probable cause.

2. The school employee, contractor, or agent has been acquitted or otherwise exonerated of the alleged misconduct.

3. The case or investigation remains open and no charges have been filed against, or indictment of, the school employee, contractor, or agent within four (4) years of the date on which the information was reported to the law enforcement agency.

Training

The school and independent contractors of the school shall provide their employees who have direct contact with children with mandatory training on child abuse recognition and reporting. The training shall include, but not be limited to, the following topics:[1] **[3] [4] [26]**

1. Recognition of the signs of abuse and sexual misconduct and reporting requirements for suspected abuse and sexual misconduct.
2. Provisions of the Educator Discipline Act, including mandatory reporting requirements. **[26]** [28]
3. Joint Operating Committee policy related to reporting of suspected abuse and sexual misconduct.
4. Maintenance of professional and appropriate relationships with students. **[27]**

Employees are required to complete a minimum of three (3) hours of training every five (5) years. [1]

Duty to Report

School employees, independent contractors, and volunteers shall make a report of suspected child abuse if they have reasonable cause to suspect that a child is the victim of child abuse under any of the following circumstances:[15]

1. The school employee, independent contractor, or volunteer comes into contact with the child in the course of employment, occupation, and the practice of a profession or through a regularly scheduled program, activity, or service.
2. The school employee, independent contractor, or volunteer is directly responsible for the care, supervision, guidance, or training of the child.
3. A person makes a specific disclosure to a school employee, independent contractor, or volunteer that an identifiable child is the victim of child abuse.
4. An individual fourteen (14) years of age or older makes a specific disclosure to a school employee, independent contractor, or volunteer that the individual has committed child abuse.

A child is not required to come before the school employee, independent contractor, or volunteer in order for that individual to make a report of suspected child abuse.[15]

A report of suspected child abuse does not require the identification of the person responsible for the child abuse.[15]

Any person who, in good faith, makes a report of suspected child abuse, regardless of whether the report is required, cooperates with an investigation, testifies in a proceeding, or engages in other action authorized by law shall have immunity from civil and criminal liability related to those actions.[29]

Any person required to report child abuse who willfully fails to do so may be subject to disciplinary action and criminal prosecution.[30]

Any person who intentionally or knowingly makes a false report of child abuse or intentionally or knowingly induces a child to make a false claim of child abuse may be subject to disciplinary action and criminal prosecution.[31]

Any person who engages in intimidation, retaliation, or obstruction in the making of a child abuse report or the conducting of an investigation into suspected child abuse may be subject to disciplinary action and criminal prosecution.[32]

The school shall not discriminate or retaliate against any person for making, in good faith, a report of suspected child abuse.[33]

Reporting Procedures

School employees, independent contractors, or volunteers who suspect child abuse shall immediately make a written report of suspected child abuse using electronic technologies (www.compass.state.pa.us/cwis) or an oral report via the statewide toll-free telephone number (1-800-932-0313). A person making an initial oral report of suspected child abuse must also submit a written electronic report within forty-eight (48) hours after the oral report. Upon receipt of an electronic report, the electronic reporting system will automatically respond with a confirmation, providing the school with a written record of the report.[15][34][35]

A school employee, independent contractor, or volunteer who makes a report of suspected child abuse shall immediately, after making the initial report, notify the school administrator and, if the initial report was made electronically, also provide the administrator with a copy of the report

confirmation. The school administrator shall then immediately notify the Executive Director or designee that a child abuse report has been made, and if the initial report was made electronically, also provide a copy of the report confirmation.[15][34][35]

When a report of suspected child abuse is made by a school employee, independent contractor, or volunteer as required by law, the school is not required to make more than one (1) report. An individual otherwise required to make a report who is aware that an initial report has already been made by a school employee, contractor, of volunteer is not required to make an additional report. The person making an initial oral report is responsible for making the follow-up written electronic report within forty-eight (48) hours, and shall provide the school administrator with a copy of the report confirmation promptly after the written electronic report has been filed. The administrator shall, in turn, provide a copy of the report confirmation to the Executive Director or designee.[15][34][35]

If the Executive Director or designee reasonably suspects that the conduct being reported involves a school safety and security incident required to be reported under law, the Executive Director or designee shall inform the law enforcement agency that has jurisdiction over the school's property, in accordance with applicable law, regulations, and Joint Operating Committee policy.[36][37][38][39][40] **[41]**

Investigation

The school administrator shall facilitate cooperation with the Department of Human Services of the Commonwealth and/or the county agency investigating a report of suspected child abuse, including permitting authorized personnel to interview the child while in attendance at the school.[15][42]

Upon notification that an investigation involves suspected child abuse by a school employee, the administrator shall immediately implement a plan of supervision or alternative arrangement that has been approved by the Executive Director for the school employee under investigation. The plan of supervision or alternative arrangement shall be submitted to the county agency for approval.[43]

Legal Footnotes

[1] **24 P.S. 1205.6**
LEGAL REFERENCE

[2] **23 Pa. C.S.A. 6301**
LEGAL REFERENCE

[3] **Pol. 333**
POLICY REFERENCE

[4] **Pol. 818**
POLICY REFERENCE

[5] 23 Pa. C.S.A. 6303
LEGAL REFERENCE

[6] 24 P.S. 111
LEGAL REFERENCE

[7] 23 Pa. C.S.A. 6344
LEGAL REFERENCE

[8] 18 Pa. C.S.A. 7508.2
LEGAL REFERENCE

[9] 42 Pa. C.S.A. 9799.12
LEGAL REFERENCE

[10] 42 Pa. C.S.A. 9799.24
LEGAL REFERENCE

[11] 42 Pa. C.S.A. 9799.55
LEGAL REFERENCE

[12] 42 Pa. C.S.A. 9799.58
LEGAL REFERENCE

[13] 22 U.S.C. 7102
LEGAL REFERENCE

[14] 23 Pa. C.S.A. 6304
LEGAL REFERENCE

[15] 23 Pa. C.S.A. 6311
LEGAL REFERENCE

[16] Pol. 302
POLICY REFERENCE

[17] Pol. 304
POLICY REFERENCE

[18] Pol. 305
POLICY REFERENCE

[19] 23 Pa. C.S.A. 6344.3
LEGAL REFERENCE

[20] 23 Pa. C.S.A. 6344.4
LEGAL REFERENCE

[21] Pol. 309
POLICY REFERENCE

[22] Pol. 916
POLICY REFERENCE

[23] 23 Pa. C.S.A. 6332
LEGAL REFERENCE

[24] 24 P.S. 111.1
LEGAL REFERENCE

[25] 20 U.S.C. 7926
LEGAL REFERENCE

[26] Pol. 317.1
POLICY REFERENCE

[27] Pol. 824
POLICY REFERENCE

[28] 24 P.S. 2070.1a
LEGAL REFERENCE

[29] 23 Pa. C.S.A. 6318
LEGAL REFERENCE

[30] 23 Pa. C.S.A. 6319
LEGAL REFERENCE

[31] 18 Pa. C.S.A. 4906.1
LEGAL REFERENCE

[32] 18 Pa. C.S.A. 4958
LEGAL REFERENCE

[33] 23 Pa. C.S.A. 6320
LEGAL REFERENCE

[34] 23 Pa. C.S.A. 6305
LEGAL REFERENCE

[35] 23 Pa. C.S.A. 6313
LEGAL REFERENCE

[36] 22 PA Code 10.2
LEGAL REFERENCE

[37] 22 PA Code 10.21
LEGAL REFERENCE

[38] 22 PA Code 10.22
LEGAL REFERENCE

[39] 24 P.S. 1306.2-B
LEGAL REFERENCE

[40] 24 P.S. 1319-B
LEGAL REFERENCE

[41] Pol. 805.1
POLICY REFERENCE

[42] 23 Pa. C.S.A. 6346
LEGAL REFERENCE

[43] 23 Pa. C.S.A. 6368
LEGAL REFERENCE

Policies are essential to school governance. We thank the JOC for its dedication and commitment to this vital process.

October 2026 Policy Updates

1. Committee - 806 - Child Abuse, 815 - Acceptable Electronic Technology Use, 818 - Contracted Services Personnel

2. First Reading - None

3. Second Reading - None

4. With Solicitor - None.

5. Reserved -

a. **000 Joint Operating Committee Procedures - None.**

b. **100 Programs- 102 - Academic Standards, 103 - ON HOLD - Discrimination/Harassment Affecting Students, 104 - ON HOLD- Discrimination/Harassment Affecting Staff, 105 - Curriculum, 105.2 - Exemption From Instruction, 113.2 - Behavior Support, 122 - Extracurricular Activities, 122.3 Noncurriculum-Related, Nonschool-Sponsored, Student-Initiated Groups. 125 - Adult Education, 140.1 - Extracurricular Participation by Charter/Cyber Charter Students, 146.1 - Trauma-Informed Approach**

c. **200 Pupils - 201 - Admission of Students, 201.1 - Deleted - Admission of Adult (Postsecondary) Students Into Secondary Programs, 202 -Eligibility of Nonresident Students, 203.1-HIV Infection, 204-Attendance, 209.2-Diabetes Management, 212-Report Student Progress, 216.1- ON HOLD- Supplemental Discipline Records, 217-Skills Certification, 218-Student Discipline, 218.1 Weapons, 218.2 Terroristic Threats, 218.3-Discipline of Student Convicted/Adjudicated of Sexual Assault, 220-Student Expression/Dissemination of Materials, 222-Tobacco and, Vaping Products, 223-Use of Motor Vehicles, 226-Searches, 227.2-Drug/Alcohol Screening, 228-Student Government, 229-Student Fundraising, 230-Public Performances by Students, 234-Pregnant/Parenting/Married Students, 236.1 Threat Assessment, 237 Electronic Devices, 246- School Wellness, 250-Student Recruitment, 252-Dating Violence, 254-Educational Opportunity for Military Children**

d. **300 Employees - None**

e. **600 Finance - 607 - Tuition Income, 626-Federal Fiscal Compliance,626.1-Travel Reimbursement-Federal Programs**

f. **700 Property - 701 Facilities Planning, 707 Use of School Facilities**

g. **800 Operations - 815.1 Use of Generative Artificial Intelligence in Education, 816 Video Camera Surveillance, 816.1 School Social Media, 819 Suicide Awareness, Prevention, and Response, 823 Opioid Antagonist, 828 Fraud, 830**

Security of Computerized Personal Information/Breach Notification, 830.1 Data Governance - Storage/Security

h. 900 Community - 901 Public Relations Objectives, 902 Publications Program, 903 Public Comment in Joint Operating Committee Meetings, 904 Public Attendance at School Events

6. On Hold - 103 - Discrimination/Harassment Affecting Students, 104 - Discrimination/Harassment Affecting Staff, 216.1- Supplemental Discipline Records, 312 - Evaluation of Executive Director

Key:

Numbers - existing JOC policy	ACP - Administrative Compensation and Benefit Plan	C/Q - Checklist and Questionnaire
AA - Articles of Agreement	CBA - Collective Bargaining Agreement	Web - UBCTS website
St Hbk - Student Handbook	Emp Hbk - Employee Handbook	

-

POLICY	RESOURCES	NEW LANGUAGE	DELETIONS/NOTES
806 - Child Abuse			
815 - Acceptable Use of Internet, Computers, and Network Resources			
818 - Contracted Services nnel			

2.B. 815 - Acceptable Electronic Technology Use

BOARD POLICY

815 Acceptable Electronic Technology Use

POLICY NUMBER	ADOPTED	REVISED	VERSION
815	3/20/2008	5/17/2012	v1
DOCUMENT STATUS	**PRINTED**		
ACTIVE	10/9/2026		

Purpose

The Joint Operating Committee recognizes the important role that computers and other forms of technology play in a student's education and in the pursuit of the school's educational goals. The Joint Operating Committee, therefore, has authorized the administration to make available computing and networked information resources, such as, the Internet, which may be used by students, faculty and staff. These resources, however, are intended to be used solely for educational purposes and to carry out the legitimate business of the school, in compliance with the Children's Internet Protection Act.

The use of network facilities shall be consistent with the curriculum adopted by the Joint Operating Committee as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.

Definitions

The terms of this policy are defined as follows:

Access - (computer) shall mean, in relation to computers to obtain entry to, or to locate, read into memory, and make ready for some operation.

Application(s) - shall mean a software program or group of programs designed for users. Applications shall include either systems software and/or applications software.

Child pornography - The term child pornography is defined under both federal and state law.[10]

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. 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.

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.[11]

Computer(s) shall mean desktops, laptops, workstations, servers, PDAs, mobile devices, telephones, tablets, or any other technology device of a similar nature that is owned, leased, or licensed by or to the school.

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

Under federal law, is any picture, image, graphic image file or other visual depiction that:[1][2]

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.

Under state law, is any depiction or representation in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it:[12]

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.

Obscene - any material or performance, if:[12]

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.

Technology - all forms of technology that is provided directly or indirectly by the school to its users, and that is: (i) owned, leased, or licensed to the school; or (ii) that is accessed by or through technology that is owned, leased, or licensed to the school.

Technology includes, but is not limited to:

- computers,
- copiers,
- printers,
- scanners,
- electronic portable devices,
- electronic peripheral devices,
- servers,
- networks,
- programs/applications,
- software,
- files,
- folders,

- data and records of any nature,
- the Internet,
- cell phones,
- mobile devices,
- pagers,
- PDAs,
- modems,
- voicemail,
- email,
- chat rooms,
- blogs,
- instant messages,
- videoconferencing,
- user group and such similar technologies.

Technology protection measure - a specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography or harmful to minors.[2]

Users - employees, students, contracted employees, and/or contractors.

User ID and/or Password - the combination of identification numbers, characters, or letters that is unique and that is assigned to an individual user to access computer devices or applications.

Vandalism - any malicious attempt to harm or destroy data of another user, Internet or other networks; this includes but is not limited to uploading or creating computer viruses.

Authority

The electronic information available to students and staff does not imply endorsement of the content by the school, nor does the school guarantee the accuracy of information received on the Internet. The school shall not be responsible for any information that may be lost, damaged or unavailable when using the network or for any information that is retrieved via the Internet.

The school shall not be responsible for any unauthorized charges or fees resulting from access to the Internet.

The school reserves the right to log network use and to monitor fileserver space utilization by users.

The Joint Operating Committee establishes that use of the Internet is a privilege, not a right; inappropriate, unauthorized and illegal use will result in cancellation of those privileges and appropriate disciplinary action.

The Joint Operating Committee shall establish a list of materials, in addition to those stated in law, that are inappropriate for access by minors.[2]

The Joint Operating Committee shall designate an online server that blocks access to visual depictions of obscenity, child pornography, or material harmful to minors.[3]

Delegation of Responsibility

The school shall make every effort to ensure that this educational resource is used responsibly by students and staff.

Administrators, teachers and other staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discriminate among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use the information to meet their educational goals.

Students and staff have the responsibility to respect and protect the rights of every other user in the school and on the Internet.

The building administrator shall have the authority to determine what is inappropriate use.

The Executive Director or designee shall be responsible for implementing technology and procedures to determine whether the school's computers are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedure shall include but not be limited to:[1][2][9]

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 Joint Operating Committee.

2. Maintaining and securing a usage log.

3. Monitoring online activities of minors/users.

The Executive Director or designee shall develop and implement administrative regulations that ensure students are educated on network etiquette and other appropriate online behavior, including but not limited to:[2]

1. Interaction with other individuals on social networking web sites and in chat rooms.

2. Cyberbullying awareness and response.[4] **[5]**

The school shall provide a copy of this policy to parents/guardians, upon written request.[3]

Guidelines

Network accounts shall be used only by the authorized owner of the account for its authorized purpose. All communications and information accessible via the network should be assumed to be private property of the school and shall not be disclosed. Network users shall respect the privacy of other users on the system.

Prohibitions

Students and staff are expected to act in a responsible, ethical and legal manner in accordance with Joint Operating Committee policy, accepted rules of network etiquette, and federal and state law. Specifically, the following uses are prohibited:

1. Facilitating illegal activity.

2. Commercial or for-profit purposes.
3. Non-work or non-school related work.
4. Product advertisement or political lobbying.
5. Hate mail, discriminatory remarks, and offensive or inflammatory communication.
6. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.
7. Access to obscene or pornographic material or child pornography.
8. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with Joint Operating Committee policy.
9. Inappropriate language or profanity.
10. Transmission of material likely to be offensive or objectionable to recipients.
11. Intentional obtaining or modifying of files, passwords, and data belonging to other users.
12. Impersonation of another user, anonymity, and pseudonyms.
13. Fraudulent copying, communications, or modification of materials in violation of copyright laws. **[6]**
14. Loading or using of unauthorized games, programs, files, or other electronic media.
15. Disruption of the work of other users.
16. Destruction, modification, abuse or unauthorized access to network hardware, software and files.
17. Quoting of personal communications in a public forum without the original author's prior consent.

Security

System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or school files. To protect the integrity of the system, the following guidelines shall be followed:

1. Employees and students shall not reveal their passwords to another individual.

2. Users are not to use a computer that has been logged in under another student's or teacher's name.

3. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.

Consequences for Inappropriate Use

The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.[7]

Illegal use of the network; intentional deletion or damage to files of data belonging to others; copyright violations; and theft of services will be reported to the appropriate legal authorities for possible prosecution.

General rules for behavior and communications apply when using the Internet, in addition to the stipulations of this policy. Loss of access and other disciplinary actions shall be consequences for inappropriate use.

Vandalism will result in cancellation of access privileges. **Vandalism** is defined as any malicious attempt to harm or destroy data of another user, Internet or other networks; this includes but is not limited to uploading or creating computer viruses.

Copyright

The illegal use of copyrighted software by students and staff is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines. **[6]** [8]

Safety

To the greatest extent possible, users of the network will be protected from harassment and unwanted or unsolicited communication. Any network user who receives threatening or unwelcome communications immediately shall bring them to the attention of a teacher or administrator. Network users shall not reveal personal information to other users on the network, including chat rooms, e-mail, Internet, etc.

Any school computer/server utilized by students and staff shall be equipped with Internet blocking/filtering software.

Internet safety measures shall effectively address the following:[2]

1. Control of access by minors to inappropriate matter on the Internet and World Wide Web.[9]
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 minor's access to materials harmful to them.

Disclaimer

Users are not permitted to create their own email disclaimer. The following disclaimer will be added to all outbound emails at the system level:

"This email and any files transmitted with it are to be treated as confidential and as such are not to be used or disclosed except for the purpose for which it has been sent. Any views or opinions presented in this email are solely those of the author and do not represent those of the Upper Bucks County Technical School. The Upper Bucks County Technical School accepts no liability for any damage caused by this e-mail. The recipient is required to indemnify the school against any claims for loss or damage caused by any viruses or otherwise."

Legal Footnotes

[1] 20 U.S.C. 6777
LEGAL REFERENCE

[2] 47 U.S.C. 254
LEGAL REFERENCE

[3] 24 P.S. 4601
LEGAL REFERENCE

[4] 24 P.S. 1303.1-A
LEGAL REFERENCE

[5] Pol. 249
POLICY REFERENCE

[6] Pol. 814
POLICY REFERENCE

[7] 24 P.S. 4604
LEGAL REFERENCE

[8] 17 U.S.C. 101
LEGAL REFERENCE

[9] **47 CFR 54.520**
LEGAL REFERENCE

[10] **18 U.S.C. 2252**
LEGAL REFERENCE

[11] **18 Pa. C.S.A. 6312**
LEGAL REFERENCE

[12] **18 Pa. C.S.A. 5903**
LEGAL REFERENCE

BOARD POLICY

815 Acceptable Use of Internet, Computers and Network Resources

POLICY NUMBER	VERSION	DOCUMENT STATUS	WORKFLOW
815	v2	UNDER-REVIEW	Committee Review

PRINTED
10/9/2026

Proposed addition Proposed deletion

Purpose

The Joint Operating Committee supports the use of the computers, the Internet, and other network resources in the ~~center (~~school~~)~~'s instructional and operational programs in order to facilitate learning, teaching, and daily operations through interpersonal communications and access to information, research, and collaboration.

The ~~center (~~school~~)~~ provides students, staff, and other authorized individuals with access to the ~~center (~~school~~)~~'s computers, electronic communication systems, and network, which includes Internet access, whether wired or wireless, or by any other means. The school provides its employees, students, and guests ("users") access to technology resources, including, but not limited to, electronic communications systems, computers, computer networks, networked devices, hardware, software, internet access, mobile devices, peripherals, copiers, and cameras.

For instructional purposes, the use of network facilities shall be consistent with the curriculum adopted by the ~~center (~~school~~)~~ as well as the varied instructional needs, learning styles, abilities, and developmental levels of students. The Joint Operating Committee supports the use of the School's technology resources to facilitate teaching and learning, to provide access to information, to aid in research and collaboration, to foster the educational mission of the School, and to carry out the legitimate business and operation of the School.

The use of the School's technology resources is for appropriate school-related educational and operational purposes and for the performance of job duties consistent with the educational mission of the School. Use for educational purposes is defined as use that is consistent with the curriculum adopted by the School as well as the varied instructional needs, learning styles, abilities, and developmental levels of students. All use for any purpose must comply with this policy and all other applicable codes of conduct, policies, procedures, and rules, and must not cause damage to the School's technology resources.

All employees and students are responsible for the lawful use of the School's technology resources in accordance with this policy. This policy is intended to ensure that all users continue to enjoy access to the School's technology resources and that such resources are utilized in an appropriate manner and for legitimate purposes.

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]

1. The production of such a 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 a 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.[2]

Computer - for purposes of this policy, ~~center (~~school~~)~~ computers include any electronic device owned or leased by the ~~center (~~school~~)~~ that has the capability to create, play, or edit text, audio and video data; transmit or receive messages, text, data or images; operate software or online applications; or provide a wired or wireless connection to the Internet.

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:[3][4]

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, it 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]

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, it lacks serious literary, artistic, political, educational, or scientific value for minors.

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

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.

School Technology Resources

School technology resources mean all technology owned, operated, and/or licensed by the School, including computers, projectors, televisions, video and sound systems, mobile devices, calculators, scanners, printers, cameras, portable hard drives, hardware, software, accounts, applications, cloud storage, routers, and networks, including the Internet.

Technology protection measure - a specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography, or harmful to minors.[4]

User

User means anyone who utilizes or attempts to utilize School technology resources while on or off School property. The term includes, but is not limited to, students, staff, parents and/or guardians, and any visitors to the School that may use School technology.

Authority

The availability of access to electronic information does not imply endorsement by the ~~center (~~school~~)~~ of the content, nor does the ~~center (~~school~~)~~ guarantee the accuracy of information received. The ~~center (~~school~~)~~ shall not be responsible for any information that may be lost, damaged, or unavailable when using the network or for any information that is retrieved via the Internet.

The ~~center (~~school~~)~~ shall not be responsible for any unauthorized charges or fees resulting from access to the Internet or other network resources.

The Joint Operating Committee declares that ~~**center (**~~**school**~~**)**~~ **Internet**, computer, and network use is a privilege, not a right. The ~~center (~~school~~)~~'s computer and network resources are the property of the ~~center (~~school~~)~~. Users shall have no expectation of privacy in anything they create, store, send, delete, **access,** receive, or display on or over the ~~center (~~school~~)~~'s Internet, computers, or network resources, including personal files. The ~~center~~

~~(~~school~~)~~ reserves the right to monitor, track, and log network access and use **on ~~center (school)~~ computers and network resources;** monitor file server~~fileserver~~ space **and file storage** utilization by ~~center (~~school~~)~~ users; or deny access to prevent unauthorized, inappropriate, or illegal activity, and may revoke access privileges and/or administer appropriate disciplinary action. The ~~center (~~school~~)~~ shall cooperate to the extent legally required with the Internet Service Provider (ISP), local, state, and federal officials in any investigation concerning or related to the misuse of the ~~center (~~school~~)~~'s Internet, computers, and network resources. [6] [7] [8]

The Joint Operating Committee requires all users to fully comply with this policy and to immediately report any violations or suspicious activities to the **building administrator** or designee.

The Joint Operating Committee establishes the following **list of subject areas as inappropriate matters~~matter~~,** in addition to those stated in law and defined in this policy, **which shall not be accessed by minors:**[4]

1. {X } **Hate speech.** [9] [10]
2. {X } Lewd, vulgar, or profane.
3. {X } Threatening.[11][12]
4. { X} Harassing or discriminatory. [9] [10] [13]
5. {X } Bullying. [14]
6. {X } **(Consisting of/Relating to) Weapons.**[15]
7. {X } Terroristic. [16]
8. { } _____ (specify others).

The ~~center (~~school~~)~~ reserves the right to restrict access to any Internet sites or **network** functions it deems inappropriate through established Joint Operating Committee policy, or the use of software and/or online server blocking/**filtering**. Specifically, the ~~center (~~school~~)~~ operates and enforces a technology protection measure(s) that blocks or filters access to

inappropriate matter by minors on its computers **and network resources** used and accessible to adults and students. The technology protection measure shall be enforced during the use of computers **and network resources** with Internet access.[3][4][17]

Upon request by students or staff, the ~~Administrative~~ Executive Director or designee shall expedite a review and may authorize the **adjustment** of **technology protection measures** to enable access to material that is blocked or **filtered** but is not prohibited by this policy. [17]

Upon request by students or staff, building administrators may authorize the temporary **adjustment** of **technology protection measures** to enable access for bona fide research or for other lawful purposes. Written permission from the parent/guardian is required prior to **adjusting** Internet blocking/filtering for a student's use. If a request for temporary **adjustment** of **technology protection measures** is denied, the requesting student or staff member may appeal the denial to the ~~Administrative~~ Executive Director or designee for expedited review.[3][18]

Delegation of Responsibility

The ~~center (~~school~~)~~ shall make every effort to ensure that this resource is used responsibly by students and staff.

The ~~center (~~school~~)~~ shall inform staff, students, parents/guardians, and other users about this policy through employee and student handbooks, posting on the ~~center (~~school~~)~~ website, and by other appropriate methods. A copy of this policy shall be provided to parents/guardians, upon written request.[17]

Users of ~~center (~~school~~)~~ networks or ~~center (~~school~~)~~-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 ~~center (~~school~~)~~ uses monitoring systems to monitor and detect inappropriate use.

{X } and tracking systems to track and recover lost or stolen equipment.

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

Administrators, teachers, and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discern among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use the information to meet their educational goals.

Students, staff, and other authorized individuals have the responsibility to respect and protect the rights of every other user in the ~~center (~~school~~)~~ and on the Internet.

Building administrators shall make initial determinations of whether inappropriate use has occurred, **and may consult with the ~~Administrative~~ Executive Director or designee and the solicitor when necessary.**

The ~~Administrative~~ Executive Director or designee shall be responsible for recommending technology and developing procedures used to determine whether the ~~center (~~school~~)~~'s computers **and network resources** are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedures shall include but not be limited to:[3] [4][19]

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 Joint Operating Committee.
2. Maintaining and securing a usage log.
3. Monitoring online activities of minors **on the ~~center (~~school~~)~~ computers and network resources.**

The ~~Administrative~~ Executive Director or designee shall develop and implement administrative regulations that ensure students are educated on network etiquette and other appropriate online behavior, including:[4]

1. Interaction with other individuals on social networking websites and in chat rooms.
2. Cyberbullying awareness and response.**[14]**[20]

Guidelines

~~Center (~~**School**~~)~~ **computers and** network accounts shall be used only by the authorized **user of the computer or** account for its approved purpose. Network users shall respect the privacy of other users on the system.

Safety

It is the ~~center (~~school~~)~~'s goal to protect users of the network from harassment and unwanted or unsolicited electronic communications. Any network user who receives threatening or unwelcome electronic communications or inadvertently visits or accesses an inappropriate site shall report such immediately to a teacher, **building** administrator, **or other appropriate staff.** Network users shall not reveal personal information to other users on the network or **Internet**, including chat rooms, email, social networking websites, etc.

Internet safety measures shall effectively address the following:[4][19]

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, **social networking websites,** 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.[21][22][23]
5. Restriction of minors' access to materials harmful to them **or which have been designated as inappropriate matter in Joint Operating Committee policy.**

Prohibitions

Users are expected to act in a responsible, ethical, and legal manner in accordance with Joint Operating Committee policy, accepted rules of network etiquette, and federal and state law **and regulations.** Specifically, the following are prohibited uses **of** ~~**center (**~~**school**~~**)**~~ **computers and/or network resources:**

1. Use of technology resources to violate the law, facilitating~~Facilitatingfacilitating~~ illegal activity, or to encourage others to do so.

2. Commercial or for-profit purposes.

3. Nonwork or non-school-related~~nonschool-related nonschool-related~~ work.

4. Product advertisement.

5. Bullying/Cyberbullying. **[14]** [20]

6. Hate mail, discriminatory remarks, **harassment,** and offensive or inflammatory communication. **[9]** **[10]** **[14]** **[24]**

7. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials. **[25]**

8. Accessing, sending, receiving, transferring, viewing, sharing, or downloading obscene, pornographic, lewd, or otherwise illegal materials, images, or photographs. **[26]**

9. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with Joint Operating Committee policy.

10. **Vulgar** language or profanity.

11. Transmission of material **that a reasonable person would know** to be offensive or objectionable to recipients.

12. Intentional obtaining or modifying of files, passwords, and data belonging to other users.

13. Impersonation of another user, anonymity, and pseudonyms.

14. Fraudulent copying, communications, or modification of materials in violation of copyright laws. **[25]**

15. Loading or **accessing** unauthorized games, programs, files, or other electronic media.

16. Disruption of the work of other users.

17. Destruction, modification, abuse, or unauthorized access to network hardware, software, **systems,** and files.

18. Accessing the Internet, ~~center (~~school~~)~~ computers, or other network resources without authorization.

19. Disabling, **adjusting,** or bypassing the Internet blocking/filtering **technology protection measure(s)** without authorization.

20. Accessing, sending, receiving, transferring, viewing, sharing, **deleting,** or downloading confidential information without authorization.
21. Use of technology resources to violate any other School policy.
22. Use of technology resources to engage in any intentional act which might threaten the health, safety, or welfare of any person or persons.
23. Use of technology resources to cause, or threaten to cause harm to others or damage to their property.
24. The use of technology resources to gamble.
25. The use of encryption software that has not been previously approved by the School.
26. Sending unsolicited mass email messages, also known as spam.
27. Use of technology resources for political lobbying or campaigning, not including student elections (e.g. student government, club officers, homecoming queen, etc.)

Security

System security is protected through the use of passwords **and/or encryption, and the ~~center (~~school~~)~~ security procedures.** Failure to adequately protect or update passwords could result in unauthorized access to personal or ~~center (~~school~~)~~ files. To protect the integrity of the system, these guidelines shall be followed:[23][27][28]

1. Employees, students**, and other authorized users** shall not reveal their passwords to another individual.

2. Users are not to use a computer that has been logged in under another **user**.

3. Any user identified as a security risk or having a history of problems with other computers **or network** systems may be denied access to the ~~center (~~school~~)~~**'s computers and** network **resources**.

Copyright

The illegal use of copyrighted materials is prohibited. Any data uploaded to or downloaded from the network **or Internet** shall be subject to fair use guidelines and applicable laws and regulations. **[25]** [29]

~~Center (~~School~~)~~ Website

The ~~center (~~school~~)~~

{ X} shall

{X } may

establish and maintain a website and shall develop and modify its web pages to present information about the ~~center (~~school~~)~~ under the direction of the ~~Administrative~~ Executive Director or designee. All **authorized** users publishing content on the ~~center (~~school~~)~~ website shall **receive appropriate training and** comply with this and other applicable Joint Operating Committee policies.

Users shall not copy or download information from the ~~center (~~school~~)~~ website and disseminate such information on unauthorized web pages without authorization from the building administrator.

Accessibility –

~~Center (~~School~~)~~ staff who maintain ~~center (~~school~~)~~ websites and web pages shall post content which is accessible to individuals with disabilities, to the same extent that it is available to other users, based on the needs of the individuals and limitations of the platform. This shall include, but is not limited to: [9] [10] [13] [30] [31][32]

1. **Including alternate text descriptions or captions for images.**
2. **Including captions for video content.**

3. **Avoiding text that is posted as an image or conveyed using only color cues.**

4. **Creating links and attachments in formats that are accessible to screen readers and other assistive technology, and may be accessed through keyboard or speech navigation.**

5. **Formatting text so that it is accessible to screen readers and other assistive technology, and may be accessed through keyboard or speech navigation.**

All ~~center (~~school~~)~~ websites shall contain clear contact information that may be used by members of the public to request accommodations or assistance.

Consequences for Inappropriate Use

Users of ~~center (~~school~~)~~ computers and network resources shall be responsible for damages to the equipment, systems, **platforms,** and software resulting from deliberate or willful acts.[17]

Illegal use of the **~~center (~~school~~)~~ computers and** network **resources**; intentional deletion or damage to files or data belonging to others; copyright violations; and theft of services shall be reported to the appropriate legal authorities for possible prosecution.

General rules **and Joint Operating Committee policies** for behavior and communications apply when using the **~~center (~~school~~)~~ computers, network resources, and** Internet, in addition to the stipulations of this policy.

Vandalism shall result in loss of access privileges, disciplinary action, and/or **referral** to legal **authorities**. **Vandalism** is defined as any malicious attempt to harm or destroy data of another user, **the ~~center (~~school~~)~~, the** Internet, or other networks; this includes but is not limited to uploading or creating computer viruses.

Failure to comply with this policy or inappropriate use of the Internet, ~~center (~~school~~)~~ network, or computers shall result in usage restrictions, loss of access privileges, disciplinary action, and/or **referral to** legal **authorities**. **[6] [7] [8]**

Unauthorized Use Prohibited

All users of School technology resources are subject to this policy. All students and staff shall be notified of and provided a copy of this policy annually. Unauthorized use, utilizing another user's School account, or exceeding one's authorization to use School technology resources is prohibited. Nothing in this policy, however, shall prevent a Parent or Guardian from assisting his or her child with the use of the School's technology resources, or from monitoring a student's use of the School's technology resources in the student's home.

Use of Personal Electronic Devices

The use of personal electronic devices on the School network is permitted only on designated networks. When a user connects a personal electronic device to a School network or School technology resources, this policy and its guidelines apply. Users are subject to the same levels of monitoring and access as if a School-owned device were being utilized. Users who connect a personal electronic device to a School network explicitly waive any expectation of privacy in the content exchanged over the School technology resources.

Privacy

The School reserves the right to monitor any user's utilization of School technology resources. Users have no expectation of privacy while using School technology resources, whether on or off School property. The School may monitor, inspect, copy, and review any and all usage of School technology resources, including information transmitted and received via the internet, to ensure compliance with this and other School policies, and state and federal law. All e-mails and messages, as well as any files stored on School technology resources, may be inspected at any time for any reason. The School may decrypt and inspect encrypted internet traffic and communications to ensure compliance with this policy.

Internet Filtering and CIPA Compliance

The School utilizes content and message filters to prevent users from accessing material through School technology resources that has been determined to be obscene, offensive, pornographic, harmful to minors, or otherwise inconsistent with the School's educational mission. The Executive Director or his/her designee shall establish a procedure for users to request that a legitimate website or educational resource not be blocked by the School's filters for a bona fide educational purpose. Such requests must be either granted or rejected within three school days pursuant to the established procedure.

The Joint Operating Committee directs that the Executive Director or his/her designee ensure that students at the high school level are educated about appropriate online behavior, including interactions via social networks and chat rooms, cyberbullying, and the disclosure of personal information.

Monitoring

School technology resources shall be periodically monitored to ensure compliance with this and other School policies, including monitoring of users' online activities. The network administrator designated by the Executive Director shall ensure that regular monitoring is completed pursuant to this section. However, the Executive Director, or his/her designee, shall also implement procedures to ensure that School technology resources are not utilized to track the whereabouts or movements of individuals, and that remotely activated cameras, audio, and/or location tracking are not utilized except where necessary to recover lost or stolen School technology, or to help locate a student or staff member in the event of an emergency.

School-Provided Resources

School technology resources may be assigned or allocated to an individual user for his or her use (e.g., individual e-mail accounts, laptop computers, etc.) Despite being allocated to a particular user, the technology resources remain the property of the School and may be revoked, suspended, restricted, or inspected at any time to ensure compliance with this and other School policies. Users do not have an expectation of privacy in any school-provided technology resource or any of its contents.

Artificial Intelligence

Artificial intelligence websites, applications, and tools may only be used on School Technology Resources in accordance with the School's Artificial Intelligence Policy, which is hereby incorporated by reference.

Disclaimer

Users are not permitted to create their own email disclaimer. The following disclaimer will be added to all outbound emails at the system level:

> "This email and any files transmitted with it are to be treated as confidential and as such are not to be used or disclosed except for the purpose for which it has been sent. Any views or opinions presented in this email are solely those of the author and do not represent those of the Upper Bucks County Technical School. The Upper Bucks County Technical School

accepts no liability for any damage caused by this email. The recipient is required to indemnify the school against any claims for loss or damage caused by any viruses or otherwise."

NOTES:

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

Federal CIPA – Children's Internet Protection Act – 47 U.S.C. Sec. 254

If ~~center (~~school~~)~~ has three (3) employee sections, change the policy cites in the policy and references.

** Check backup, particularly any User Agreements included in handbooks, to determine whether or not to add the option for tracking and recovering lost or stolen equipment – if the ~~center (~~school~~)~~ has not disabled this type of tracking system, the language should be included in the policy to put users on notice.

PSBA Revision 10/23 © 2023 PSBA

Legal Footnotes

[1] 18 U.S.C. 2256
LEGAL REFERENCE

[2] 18 Pa. C.S.A. 6312
LEGAL REFERENCE

[3] 20 U.S.C. 7131
LEGAL REFERENCE

[4] 47 U.S.C. 254
LEGAL REFERENCE

[5] 18 Pa. C.S.A. 5903
LEGAL REFERENCE

[6] Pol. 218 — Student Discipline
POLICY REFERENCE

[7] Pol. 233 — Suspension and Expulsion
POLICY REFERENCE

[8] Pol. 317 — Conduct/Disciplinary Procedures
POLICY REFERENCE

[9] Pol. 103 — Discrimination/Title IX Sexual Harassment Affecting Students
POLICY REFERENCE

[10] Pol. 104 — Discrimination/Title IX Sexual Harassment Affecting Staff
POLICY REFERENCE

[11] 24 P.S. 1302-E
LEGAL REFERENCE

[13] Pol. 103.1 — Nondiscrimination — Qualified Students With Disabilities
POLICY REFERENCE

[14] **Pol. 249 — Bullying/Cyberbullying**
POLICY REFERENCE

[16] **Pol. 218.2 — Terroristic Threats**
POLICY REFERENCE

[17] **24 P.S. 4604**
LEGAL REFERENCE

[18] **24 P.S. 4610**
LEGAL REFERENCE

[19] **47 CFR 54.520**
LEGAL REFERENCE

[20] **24 P.S. 1303.1-A**
LEGAL REFERENCE

[25] **Pol. 814 — Copyright Material**
POLICY REFERENCE

[26] **Pol. 237 — Electronic Devices**
POLICY REFERENCE

[29] **17 U.S.C. 101 et seq**
LEGAL REFERENCE

[30] **42 U.S.C. 12101 et seq**
LEGAL REFERENCE

[31] **29 U.S.C. 794**
LEGAL REFERENCE

[32] **28 CFR 35.160**
LEGAL REFERENCE

2.C. 818 - Contracted Services Personnel

BOARD POLICY

818 Contracted Services Personnel

POLICY NUMBER	ADOPTED	VERSION	DOCUMENT STATUS
818	6/19/2025	v1	ACTIVE

PRINTED
10/9/2026

Purpose

In its effort to provide cost-effective programs, the Joint Operating Committee may need to use outside independent contractors for a variety of purposes. The school is required to ensure that such contractors comply with certain legal requirements regarding contractor employees involved in the delivery of services to the school. This policy is adopted to outline those requirements and the manner in which the school shall direct and monitor contractor compliance.

Definitions

For purposes of this policy, **contractor employee** shall include an individual who:

1. Is employed or offered employment by an independent contractor or a subcontractor of an independent contractor, or is an individual independent contractor; and
2. Has or will have direct contact with children.

Direct Contact with Children - the possibility of care, supervision, guidance or control of children or routine interaction with children.[1]

For purposes of this policy, **independent contractor** shall mean an individual or entity that contracts with the school to provide services.

Authority

The school is required by law to ensure that independent contractors and contractor employees comply with the mandatory background check requirements for criminal history and child abuse certifications, the employment history review requirement, and the arrest and conviction reporting requirements.[2][3][4]

Guidelines

Prior to using contracted services, a written contractual agreement shall be entered into between the school and the independent contractor and maintained centrally by the school in a manner similar to that for other contracts. Requests for proposals, bid specifications for proposals and resulting contracts shall specify the following:

1. Mandatory requirements for criminal history background checks, child abuse certifications, employment history reviews, and arrest and conviction reporting for contracted services involving direct contact with children, as mandated by law and set forth in this policy.[5]

2. A requirement that all contracted transportation providers provide a program of drug and alcohol testing for covered drivers. A covered driver shall include any contractor employee who drives, operates or is in the actual physical control or movement of a school bus or a commercial vehicle owned, leased or operated by the independent contractor in connection with school programs and services.[6][7][8][9][10]

3. That failure to comply with this policy and the requirements for criminal history background checks and child abuse certifications, employment history reviews, and required reporting of employee arrests, convictions or other misconduct by an independent contractor or contractor employee shall be grounds for termination of the contract.

The Executive Director or designee shall review all information provided pursuant to this policy and determine if information is disclosed that precludes employment or continued service of an independent contractor or contractor employee.[2][3][4][5][11]

Information submitted by an independent contractor or contractor employee in accordance with this policy shall be maintained centrally in a manner similar to that for school employees.

Pre-Employment Requirements

Employment History Review -

Independent contractors shall conduct an employment history review, in compliance with state law, prior to assignment of a contractor employee to perform work for the school in a position or assignment involving direct contact with children. The independent contractor may use the information for the purpose of evaluating an applicant's fitness to be hired or for continued employment of a current contractor employee and may report the information as permitted by law.[4]

Independent contractors shall inform the school, in writing, upon receipt of an affirmative response to any of the abuse and sexual misconduct background questions for a contractor employee. If the school objects to the assignment, the independent contractor may not assign the contractor employee to the school.[4]

Independent contractors shall, upon request, provide the school to which a contractor employee is assigned access to the employee's employment history review records.

Criminal History -

Prior to assignment of contractor employees to perform work for the school in a position or assignment involving direct contact with children, contractor employees shall submit an official child abuse clearance statement and state and federal criminal history background checks (certifications) as required by law.[2][3]

Contractor employees shall report, on the designated form, all arrests and convictions as specified on the form. Contractor employees shall likewise report arrests and/or convictions that occur subsequent to initially submitting the form. Failure to accurately report such arrests and convictions may subject the individual to denial of employment/contract, termination if already hired/contracted, and/or criminal prosecution.[3]

Tuberculosis Test -

Contractor employees providing services for students shall undergo a test for tuberculosis in accordance with the regulations and guidance of the Pennsylvania Department of Health.[12][13]

Arrest and Conviction Reporting Requirements

All independent contractors shall adopt policies and procedures that require their employees, who are providing services to the school and who have direct contact with children, to notify the independent contractor, in writing, within seventy-two (72) hours of the occurrence, of an arrest or conviction required to be reported by law. Contractor employees shall also be required to report to the independent contractor, within seventy-two (72) hours of notification, that the employee has been named as a perpetrator in a founded or indicated report pursuant to the Child Protective Services Law. The policies and procedures shall also include the provision that the failure on the part of contractor employees to make such a timely notification shall subject them to disciplinary action, including termination.[3][11]

If the independent contractor receives notice of such arrest or conviction or that the contractor employee has been named as a perpetrator in a founded or indicated report, from either the contractor employee or a third party, the independent contractor shall immediately report, in writing, that information to the Executive Director or designee.

The independent contractor shall immediately require a contractor employee to submit new certifications when there is a reasonable belief that the employee was arrested for or has been convicted of an offense required to be reported by law, was named as a perpetrator in a founded or indicated report, or has provided written notice of such occurrence.[3][11]

Contractor employees who provide transportation services shall immediately notify the independent contractor and the school's transportation supervisor of any traffic citations or the suspension, revocation or cancellation of operating privileges.[14]

Educator Misconduct

If the Executive Director reasonably suspects that conduct being reported involves an incident required to be reported under the Educator Discipline Act, the Executive Director or designee shall notify the Pennsylvania Department of Education, in accordance with applicable law, regulations and Joint Operating Committee policy 317.1.[15] **[16]**

Training

Independent contractors shall provide their employees who have direct contact with children with mandatory training on child abuse recognition and reporting. The training shall include, but not be limited to, the following topics:[1]

1. Recognition of the signs of abuse and sexual misconduct and reporting requirements for suspected abuse and sexual misconduct.
2. Provisions of the Educator Discipline Act, including mandatory reporting requirements.[17]
3. School policy related to reporting of suspected abuse and sexual misconduct. **[18]**
4. Maintenance of professional and appropriate relationships with students. **[19]**

Employees of independent contractors who have direct contact with children are required to complete a minimum of three (3) hours of training every five (5) years.[1]

Contractor employees shall attend orientation and training sessions, as appropriate to the nature of their service. When training is provided for school employees relating to the legal obligations of employers and educational institutions, consideration shall be given to which contractor employees should also receive that training.

Child Abuse Reporting

All contractor employees who have reasonable cause to suspect that a child is the victim of child abuse shall make a report of suspected child abuse in accordance with applicable law, Joint Operating Committee policy and administrative regulations. **[18]** [20]

Confidentiality

No contractor employee shall be permitted access to confidential student information unless the school has determined that such access is necessary for the contractor employee to fulfill his/her responsibilities. Contractor employees with access to confidential student information shall maintain the confidentiality of that information in accordance with Joint Operating Committee policies and procedures and applicable law. If a contractor employee has questions about the confidentiality of student information, the contractor employee should consult with the building administrator. **[21]** **[22]**

Legal Footnotes

[1] 24 P.S. 1205.6
LEGAL REFERENCE

[2] 23 Pa. C.S.A. 6344
LEGAL REFERENCE

[3] 24 P.S. 111
LEGAL REFERENCE

[4] 24 P.S. 111.1
LEGAL REFERENCE

[5] 55 PA Code 3490.132
LEGAL REFERENCE

[6] 49 CFR Part 382
LEGAL REFERENCE

[7] 67 PA Code 71.3
LEGAL REFERENCE

[8] 75 Pa. C.S.A. 1612
LEGAL REFERENCE

[9] 75 Pa. C.S.A. 3802
LEGAL REFERENCE

[10] Pol. 810.1
POLICY REFERENCE
Referenced policy is not available in this policy book.

[11] 23 Pa. C.S.A. 6344.3
LEGAL REFERENCE

[12] 24 P.S. 1418
LEGAL REFERENCE

[13] 28 PA Code 23.44
LEGAL REFERENCE

[14] 75 Pa. C.S.A. 1606
LEGAL REFERENCE

[15] 24 P.S. 2070.9a
LEGAL REFERENCE

[16] Pol. 317.1
POLICY REFERENCE

[17] 24 P.S. 2070.1a
LEGAL REFERENCE

[18] Pol. 806
POLICY REFERENCE

[19] Pol. 824
POLICY REFERENCE

[20] 23 Pa. C.S.A. 6311
LEGAL REFERENCE

[21] Pol. 113.3
POLICY REFERENCE

[22] Pol. 216
POLICY REFERENCE

3. **First Reading**
4. **Second Reading**
5. **Next Scheduled Meeting Date**
6. **Adjournment**