

782 Springdale Drive, Exton, Pennsylvania 19341 • Phone: 484-266-1000 • www.wcasd.net

### Dear Retiree Substitute Volunteer Applicant:

Thank you for your interest in participating in the West Chester Area School District Senior Citizen Tax Credit Community Service Program. In return for your volunteer services, you will be entitled to a rebate of property taxes in accordance with the Retiree Substitute Volunteer Program (RSVP) guidelines.

### Enclosed please find:

- Retiree Substitute Volunteer Program (RSVP) Application
- WCASD Policy 348 Harassment Policy
- WCASD Policy 352 & 352AG3 Non-Employee Internet Policy Form
- WCASD Policy 815.4 Use of Personal Technology and Electronic Devices
- Sign off District Policy Review
- WCASD Emergency Medical Card
- Retiree Substitute Volunteer Program Guidelines & Monthly Volunteer Log
- Map of District Buildings

In order to process your Retiree Substitute Volunteer Program application, we must have:

- Your completed application (be sure all information is provided including Tax Parcel Number)
- A copy of your Social Security card
- A current Act 34 Pennsylvania Criminal Record Check
- A current Act 151 Pennsylvania Child Abuse History Clearance
- A current Act 114 Federal Criminal History Check
- Completed and Signed District Policy Review and Form 352AG3
- Completed WCASD Emergency Medical Card
- Results from Tuberculin Test taken within the past year (from your private physician)

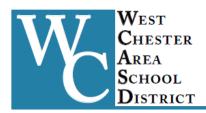
Applicants interested in this program must call the Human Resources Department at 484-266-1007 to request a packet of information. Please call if you have any questions or need assistance with any of the forms listed above.

ALL BACKGROUND CHECKS ARE GOOD FOR ONE YEAR FROM THE DATE OF ISSUE.

Sincerely,

Jeffrev G. Ulmer

**Director of Human Resources** 



782 Springdale Drive, Exton, Pennsylvania 19341 • Phone: 484-266-1000 • www.wcasd.net

# APPLICATION FOR RETIREE SUBSTITUTE VOLUNTEER PROGRAM

Position Applying for:	Retiree Substitute Volu	nteer Program	Date you	can start:
age by December 31st of	the Retiree Substitute Vol the year in which you vol nis requirement?		SVP), you 1	must be at least 62 years of
		SONAL DATA be or print in ink)		
Name in Full: (Last Nam	ne First)		Social	Security #
Street Address:			_ Cell/Hon	ne Phone #
City, State, Zip				
Last Previous Address:				
Tax Parcel Number: (MUST BE number from your tax bill, pleas		ax parcel number to appl	y proper rebate.	If you cannot obtain the tax parcel
Tax Parcel #				
Please list your skills, pe	ervious job background, ho	obbies, or interests:		
	RE	EFERENCES		
Please list (3) references below:		T		
Full Name	Business	Complete A	ddress	Cell/Home/Business Phone
1.				
2.				
3.				

### GENERAL BACKGROUND INFORMATION

You must give complete answers to all questions. If you answer "Yes" to any question, you must list all offenses and for each conviction provide data of conviction and disposition regardless of the date or location of occurrence. Conviction of a criminal offense is not a bar to employment in all cases. Each case is considered on its merits. Your answers will be verified with appropriate police records.

<u>Criminal Offense</u> includes felonies, misdemeanors, summary offenses and convictions resulting from a plea of "nolo con-tendere" (no contest).

<u>Conviction</u> is an adjudication of guilt and includes determinations before a court, a district justice or a magistrate which results in a fine, sentence, or probation.

You may omit minor traffic violations, offenses committed before your 18th birthday which were adjudicated in juvenile court or under a Youth Offender law, and any convictions which have been expunged by a court or for which you successfully completed an Accelerated Rehabilitative Disposition program.

	_	
Were you ever convicted of a criminal offense?	YES	NO 🗌
Are you currently under charges for a criminal offense?	YES	NO 🗌
Have you ever forfeited bond or collateral in connection with a criminal offense?	YES	NO 🗌

NOTE: If you answered "Yes" to any of the above questions, please provide a detailed explanation on a separate sheet of paper, including dates, and attach it to this application. Please print and sign your name on the sheet and include your social security number.

### ACT 34 COMPLIANCE (PA State Criminal Record Check)

Each Pennsylvania resident must submit with his/her application a copy of a report of Criminal History Record information from the Pennsylvania State Police or a statement from the Pennsylvania State Policy that the State Police Central Repository contains no such information relating to that person. The criminal record history report must be no more than one (1) year old. The applicant MUST submit the ORIGINAL report prior to start.

### ACT 151 (Pennsylvania Child Abuse History Clearance)

Each volunteer must submit with his/her application a copy of an official clearance statement obtained from the Pennsylvania Department of Public Welfare or a statement from the Department of Public Welfare that no record exists. The clearance statement must be no more than one (1) year old. The applicant MUST submit the ORIGINAL report prior to start.

### ACT 114 (Federal Criminal History Check)

Each resident must submit with his/her application an original copy of the FBI results or a copy of the registration receipt clearly showing the Registration/TCN number. The clearance must be no more than one (1) year old. The resident MUST submit the FBI information prior to start.



Book Policy Manual
Section 300 Employees

Title Unlawful Harassment

Number 348

Status Active

Adopted August 1, 2015
Last Reviewed June 22, 2015

### **Purpose**

The Board is committed to maintaining a working environment free from sexual harassment and harassment based on race, color, religion, national origin/ethnicity, disability, medical condition, marital status, age, sex, sexual orientation, or genetic information, hereinafter referred to as protected characteristics. Therefore, the purpose of this policy is to prohibit sexual harassment and harassment based on any of the protected characteristics at school or any school-sponsored event/activity.

### **Authority**

It shall be a violation of this policy for school personnel to sexually harass a student, school personnel or other person, or harass a student, school personnel, or other person based on any of the protected characteristics. Further, it shall be a violation of this policy for school personnel to assist or encourage or knowingly permit sexual harassment or harassment based on a protected characteristic of a student, school personnel, or other person. The Board encourages employees and other persons who have been harassed or witnessed harassment to promptly report such incidents to the designated administrators.[1][2][3][4][5]

### **Definitions**

**Harassment** based on any of the protected characteristics (unlawful harassment) consists of verbal, written, graphic or physical conduct relating to an individual's race, color, religion, national origin/ethnicity, disability, medical condition, marital status, age, sex, sexual orientation, or genetic information when the conduct:[3][4]

- 1. Creates an intimidating, threatening, or abusive work environment or educational environment.
- 2. Has the purpose or effect of substantially or unreasonably interfering with an individual's work performance or learning performance.
- 3. Is sufficiently severe, persistent or pervasive that it affects an individual's ability to perform job functions or academic functions.
- 4. Otherwise adversely affects an individual's employment opportunities or educational opportunities.

Examples of conduct which may constitute **harassment** based on a protected characteristic, if it meets the immediately preceding definition, include but are not limited to:

- 1. Graffiti containing racially offensive language.
- 2. Name calling, jokes, or spreading false or scandalous information.
- 3. Physical acts of aggression or hostile acts against a person or his/her property because of that person's race, color, religion, national origin/ethnicity, disability, medical condition, marital status, age, sex, sexual orientation, or genetic information.
- 4. Written or graphic material which is posted or circulated and which intimidates or threatens, or which is intended to intimidate or threaten, a person based on that person's race, color, religion, national origin/ethnicity, medical condition, disability, marital status, age, sex, sexual orientation, or genetic information.

**Sexual harassment** consists of an unwelcome sexual advance, request for sexual favor, and other inappropriate verbal, written, graphic, or physical conduct or communication of a sexual nature when:

[6]

- 1. Submission to that conduct or communication is made a term or condition, either explicitly or implicitly, of an individual's continued employment or educational opportunity.
- 2. Submission to or rejection of the conduct or communication by an individual is used as a factor in employment decisions affecting that individual.
- 3. That conduct or communication is sufficiently severe, persistent, or pervasive that it substantially or unreasonably interferes with an individual's job or academic performance or creates an intimidating, hostile or offensive working environment (i.e. the conduct is sufficiently serious to limit an employee's ability to participate in or benefit from the work or academic environment).

Examples of conduct which may constitute **sexual harassment**, if it meets the immediately preceding definition, include but are not limited to:

- 1. Unwelcome sexual physical contact of an individual's body or clothes.
- 2. Unwelcome ongoing or repeated sexual flirtation or propositions, or remarks.
- 3. Sexual slurs, leering, epithets, threats, verbal abuse, derogatory comments, or sexually degrading descriptions.
- 4. Graphic comments about an individual's body.
- 5. Sexual jokes, notes, stories, drawings, gestures, or pictures.
- 6. Spreading sexual rumors.
- 7. Displaying sexual objects, pictures, cartoons, or posters.

For purposes of this policy, **school personnel** shall include any School Board member, school employee, agent, volunteer, contractor, or other person subject to the supervision and control of the district.

### **Guidelines**

### Complaint Procedure

Formal Procedure -

File Report – Any school personnel or other person who believes that s/he has been the victim or
witness of sexual harassment or harassment based on a protected characteristic by a student or
school personnel should report the alleged harassment as soon as possible. Further, any student
who has knowledge of such conduct which may constitute prohibited harassment should report
any such conduct to one of the Compliance Officers designated in Section 5 of this procedure or

to any school personnel. Any school personnel who has knowledge of conduct which may constitute prohibited harassment shall immediately report the alleged harassment to one of the Compliance Officers designated in this policy.

The reported complaint of harassment should be made orally and/or in writing (348-AG-1 Complaints of Unlawful Harassment Report Form – Employees) with either the building principal or one of the Compliance Officers designated in this policy. The principal shall immediately forward any report of alleged prohibited harassment to the Compliance Officer. Any complaint that involves the Compliance Officer or principal shall be reported to the Superintendent.

The complaint, the identity of the complainant, and the identity of the person accused of harassment will be disclosed only to the extent necessary to fully investigate the complaint and only when such disclosure is permitted by law.

Additionally, a complainant who wishes to remain anonymous shall be advised that such confidentiality may limit the district's ability to fully respond to the complaint.

2. <u>Investigation</u> – Upon receipt of a report of alleged harassment, the Compliance Officer shall promptly authorize or undertake an investigation. The investigation may be conducted by school personnel, or a third party designated by the district to perform that function. The investigation shall be completed as soon as practicable, which generally should be not later than fourteen (14) calendar days after receipt of the report to the Compliance Officer. Upon receiving the complaint, the Compliance Officer shall acknowledge receipt of the complaint by giving written notice to the complainant that the complaint has been received. Also upon receiving the complaint, the Compliance Officer shall determine whether interim measures should be taken pending the outcome of the investigation. Such interim measures may include, but are not limited to, taking measures to reduce or eliminate contact between the alleged harasser and the complainant and, in cases reasonably believed to involve potential criminal conduct, determining whether law enforcement officials should be notified. If the Compliance Officer determines that more than fourteen (14) days will be required to investigate the complaint, the complainant and the accused shall be notified of the reason for the extended investigation and of the date by which the investigation will be concluded.

The investigation may consist of interviews with the complainant, the alleged harasser, and any others who may have knowledge of the alleged harassment or the circumstances giving rise to the complaint. The investigation may also consist of the inspection of any documents or other information deemed relevant by the investigator.

In determining whether alleged conduct constitutes a violation of this policy, the Compliance Officer, and any investigator appointed by the Compliance Officer, shall consider, at a minimum: (i) the surrounding circumstances; (ii) the nature of the behavior; (iii) incidents of past or continuing patterns of behavior; (iv) how often the conduct occurred; (v) the relationship of the alleged perpetrator to the alleged victim (e.g., whether the alleged perpetrator was in a position of authority over the alleged victim); (vi) the location of the alleged harassment; (vii) the ages of the parties and (viii) the context in which any alleged incident(s) occurred. Whether a particular action or incident constitutes a violation of this policy requires a case-by-case determination based on all of the facts and circumstances revealed after a complete and thorough investigation.

The Compliance Officer shall issue a written report to the Superintendent upon completion of the investigation. If the complaint involves the Superintendent, then the report shall be sent to the Board. The report shall include the Compliance Officer's determination of whether and how this policy was violated and recommendations for disciplinary and/or corrective action, if any.

All employees shall cooperate with any investigation of alleged harassment conducted under this policy or by any investigating local, state or federal agency.

3. Action by Superintendent – Within five (5) calendar days of actual receipt of the Compliance Officer's report, the Superintendent or his/her designee shall issue a decision regarding whether and how this policy was violated. This decision must be provided in writing to the complainant and the person accused of harassment. If the Superintendent or his/her designee determines that prohibited harassment occurred, prompt, appropriate action shall be taken to address and remedy the violation as well as to prevent any recurrence. Such action may include discipline, up to and including expulsion or discharge Whether or not the Superintendent or his/her designee determines that prohibited harassment occurred, the Superintendent or his/her designee may determine that building, group, or individual training be conducted and/or that the complainant and/or harasser be invited to receive counseling.

- 4. <u>Appeal</u> If the Superintendent or his/her designee determines that no prohibited harassment occurred, the complainant may appeal this finding to the Board within five (5) calendar days of receiving the decision. Any such appeal must be in writing and filed with the Superintendent, who shall forward the appeal and investigation record to the Board. The Board shall make a good faith effort to make a decision within thirty (30) calendar days of receiving the record. The Board may ask for oral or written argument from the complainant, the Superintendent, the person accused of harassment, and/or other person(s).
  - If the Superintendent or his/her designee determines that prohibited harassment occurred and discipline is imposed, the disciplined person may appeal the disciplinary sanction in the same manner as any other such sanction would be appealed.
- 5. <u>Compliance Officer and Alternate Compliance Officer</u> The Board has designated the Director of Secondary Education as the Compliance Officer described within this policy. Complaints of harassment may also be made to the Alternate Compliance Officer, the Director of Human Resources. The Alternate Compliance Officer shall act as the Compliance Officer for any complaint received by him/her.[7]

The responsibilities of the Compliance Officer or Alternate Compliance Officer shall include the following:

- a. Receive reports or complaints of harassment.
- b. Oversee the investigation of any alleged harassment.
- c. Assess the training needs of the district in connection with this policy.
- d. Arrange necessary training to achieve compliance with this policy.
- e. Ensure that any harassment investigation is conducted by an impartial and appropriately trained investigator.
- f. Take all reasonable measures to protect the alleged victim and others during the investigation.

### Informal Procedure -

If the complainant and the person accused of harassment agree, they may arrange with the Compliance Officer to attempt to resolve the complaint informally with the help of a counselor, teacher, or administrator, or other qualified third party. In that event they shall each be informed by the Compliance Officer that they have the right to abandon the informal procedure at any time in favor of the initiation or continuation of the formal complaint procedure set forth in this policy. If the complainant and the person accused of harassment are successful in resolving the complaint informally, the Compliance Officer shall keep a written record of the agreement between the parties.

### <u>Miscellaneous</u>

### Retaliation -

Retaliation against students, school personnel, or other persons who report harassment pursuant to this policy or who participate in any related proceeding is prohibited. The Board deems retaliatory acts as harmful as harassing acts and shall take appropriate action against students or school personnel who retaliate against any student, school personnel, or other person who reports alleged harassment or participates in related proceedings. Such action may include discipline, up to and including expulsion or discharge or civil action.

### Right to Alternative Complaint Procedure -

Nothing in this policy shall deny the right of any individual to pursue other avenues of recourse to address concerns relating to prohibited harassment including initiating civil action, filing a complaint with outside agencies, or seeking redress under state or federal law.

### Dissemination of Policy -

All employees shall receive a copy of this policy when they are hired and annually thereafter. In addition, this policy shall be posted in every district building housing student classrooms or school personnel offices and disseminated to students, parents/guardians, independent contractors, vendors, and the public on an annual basis.

### False Charges -

School personnel who knowingly make false charges of harassment or retaliation shall be subject to disciplinary action, up to and including expulsion or discharge or civil action.

Legal 1. 20 U.S.C. 1681 et seq

2. 42 U.S.C. 2000e et seq

3. 42 U.S.C. 2000ff et seq

4. 29 CFR 1606.8

5. 43 P.S. 951 et seq

6. 29 CFR 1604.11

7. Pol. 104

Pol. 000

Pol. 317



Book Policy Manual
Section 300 Employees

Title Staff Acceptable Use of Internet, Computers and Network Resources

Number 352

Status Active

Adopted August 1, 2015
Last Revised March 27, 2017

### **Purpose**

Digital technology has radically changed the way the world communicates and accesses information. The Internet and mobile telecommunications represent powerful educational and productivity resources unlike anything that has preceded them.

The district provides staff and other authorized individuals with access to the district's computers, electronic communication systems and network, which includes Internet access, whether wired or wireless, or by any other means.

For all users, the district-provided computers, Internet and other network resources must be used for district business or academic purposes.

For instructional purposes, the use of network facilities shall be consistent with the curriculum adopted by the district as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.

### **Definitions**

**Child pornography -** under federal law, child pornography is defined as 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 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, **child pornography** is defined as 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]

**Harmful to minors -** under federal law, harmful to minors is defined as 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 lacks serious literary, artistic, political or scientific value as to minors.

Under state law, **harmful to minors** is defined as 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 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.

**Incidental personal use** - use of the district's computers, Internet and other network resources by an employee for occasional, personal research and communications.

**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]

### Authority

The availability of access to electronic information does not imply endorsement by the district of the content, nor does the district guarantee the accuracy of information received. The district 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 district shall not be responsible for any unauthorized charges or fees resulting from access to the Internet or other network resources.

The Board declares that computer and network use is a privilege, not a right. The district's computer and network resources are the property of the district. Users shall have no expectation of privacy in anything they create, store, send, delete, receive or display on or over the district's Internet, computers or network resources, including personal files or any use of the district's Internet, computers or network resources. The district reserves the right to monitor, track, and log network access and use; monitor fileserver space utilization by district users; or deny access to prevent unauthorized, inappropriate or illegal activity and may revoke access privileges and/or administer appropriate disciplinary action. The district 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 district's Internet, computers and network resources.[6][7][8]

The purpose of the Acceptable Use Policy is to provide information, not to exclude anyone. However, the district reserves the right to prioritize the use of systems and does not intend to create a First

Amendment forum for free expression purposes.

The Board requires all users to fully comply with this policy and to immediately report any violations or suspicious activities to the Superintendent or designee.

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.[3] [4][9]

Upon request by staff, the Superintendent or designee shall expedite a review and may authorize the disabling of Internet blocking/filtering software for specific websites to enable access to material that is blocked through technology protection measures but is not prohibited by this policy 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 is denied, the requesting staff member may appeal the denial to the Superintendent or designee for expedited review.[3][9][10]

### **Delegation of Responsibility**

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

The district shall inform staff and other users about this policy through employee handbooks, posting on the district website, and by other appropriate methods. A copy of this policy shall be provided to a staff member, upon written request.[9]

Users of district networks or district-owned equipment shall read and understand the provisions of this policy, and be aware that the district uses monitoring systems to monitor and detect inappropriate use and tracking systems to track and recover lost or stolen equipment.

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 district and on the Internet.

Building administrators shall make initial determinations of whether inappropriate use has occurred.

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: [3][4][11]

- 1. Utilizing a technology protection measure that blocks or filters Internet access for staff to certain visual depictions that are obscene, child pornography, harmful to students with respect to use by minors, or determined inappropriate for use by students by the Board.
- 2. Maintaining and securing a usage log.
- 3. Monitoring online activities of staff.

The Superintendent or designee shall develop and implement administrative guidelines that ensure that staff members are educated on network etiquette and safe and appropriate online behavior, including:[4]

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

2. Cyberbullying awareness and response.[12][13]

Education will be provided through such means as professional development, the district website, and other materials.

### **Guidelines**

Network accounts shall be used only by the authorized owner of the account for its approved purpose. Network users shall respect the privacy of other users on the system.

### Incidental Personal Use

Incidental personal use shall be permitted for employees, as defined in this policy. Personal use must comply with this policy and all other applicable policies, procedures and rules, as well as ISP, local, state and federal laws, and may not interfere with the employee's job duties and performance, with the system operations, or with other system users.

### Safety

It is the district'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 or administrator. Network users shall not reveal personal information to other users on the network, including chat rooms, email, social networking websites, etc.

Internet safety measures shall effectively address the following: [4][11]

- 1. Control of access by students to inappropriate matter on the Internet and World Wide Web.
- 2. Safety and security of students when using electronic mail, chat rooms, and other forms of direct electronic communications.
- 3. Prevention of unauthorized online access by students, including "hacking" and other unlawful activities.
- 4. Unauthorized disclosure, use, and dissemination of personal information regarding students.
- 5. Restriction of students' access to materials harmful to them.

### **Prohibitions**

Staff members are expected to act in a responsible, ethical and legal manner in accordance with district 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. Nonwork or nonschool related work.
- 4. Product advertisement or political lobbying.
- 5. Bullying/Cyberbullying.[12][13]
- 6. Hate mail, discriminatory remarks, and offensive or inflammatory communication.
- 7. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.

8. Accessing, sending, receiving, transferring, viewing, sharing or downloading obscene, pornographic, lewd, or otherwise illegal materials, images or photographs.[14]

- 9. Access by students to material that is harmful to minors or is determined inappropriate for minors in accordance with Board policy.
- 10. Inappropriate language or profanity.
- 11. Transmission of material likely 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. [15]
- 15. Loading or using of 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 and files.
- 18. Accessing the Internet, district computers or other network resources without authorization.
- 19. Disabling or bypassing the Internet blocking/filtering software without authorization.
- 20. Accessing, sending, receiving, transferring, viewing, sharing or downloading confidential information without authorization.

### 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 district files. To protect the integrity of the system, these guidelines shall be followed:

- 1. Staff members shall not reveal their passwords to another individual.
- 2. Staff members are not to use a computer that has been logged in under another user's name.
- 3. Any staff member identified as a security risk or having a history of problems with other computer systems may be denied access to the network.

### Copyright

The illegal use of copyrighted materials is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines and applicable laws and regulations.[15][16]

### **District Website**

The district shall establish and maintain a website and shall develop and modify its web pages to present information about the district under the direction of the Superintendent or designee. All users publishing content on the district website shall comply with this and other applicable district policies and administrative guidelines.

Users shall not copy or download information from the district website and disseminate such information on unauthorized web pages without authorization from the building principal.

### Consequences for Inappropriate Use

Staff members shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.[9]

Illegal use of the network; 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 for conduct and communications apply when using the Internet, in addition to the stipulations of this policy. All network users are responsible for complying with all applicable Board policies, administrative guidelines and regulations, and federal, state and local law while utilizing district equipment, network resources and Internet.[6]

Vandalism shall result in loss of access privileges, disciplinary action, and/or legal proceedings. **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.

Failure to comply with this policy or inappropriate use of the Internet, district network or computers shall result in usage restrictions, loss of access privileges, disciplinary action, and/or legal proceedings. [7][8]

### **Guest Accounts**

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

An open guest network with filtered access to the Internet, but no other network services, may be maintained at the discretion of the Superintendent or designee. Persons accessing the Internet through the open guest network do so at their own risk. The district assumes no responsibility for any damage to the guest's device or charges incurred resulting from connectivity. Guests using the open network agree to all applicable provisions of this policy and other applicable district policies.

Access to all data on, taken from, or compiled using any part of the district's network is subject to inspection and discipline or legal action by the district. District information placed on users' personal computers, networks, Internet, and electronic communications systems is subject to access by the district. The district reserves the right to legally access users' personal equipment for district information. The district reserves the right to monitor, track, and log network access and use; monitor fileserver space utilization; maintain usage logs; and monitor online activity.

Legal

- 1. 18 U.S.C. 2256
- 2. 18 Pa. C.S.A. 6312
- 3. 20 U.S.C. 6777
- 4. 47 U.S.C. 254
- 5. 18 Pa. C.S.A. 5903
- 6. Pol. 218
- 7. Pol. 233
- 8. Pol. 317
- 9. 24 P.S. 4604
- 10. 24 P.S. 4610
- 11. 47 CFR 54.520
- 12. 24 P.S. 1303.1-A
- 13. Pol. 249
- 14. Pol. 237
- 15. Pol. 814
- 16. 17 U.S.C. 101 et seq
- 24 P.S. 4601 et seq
- Pol. 103
- Pol. 103.1
- Pol. 104
- Pol. 218.2
- Pol. 220
- Pol. 248
- Pol. 348
- Pol. 815.1
- Pol. 815.2
- Pol. 815.3
- Pol. 815.4

# WEST CHESTER AREA SCHOOL DISTRICT

ADMINISTRATIVE GUIDELINE

ADOPTED: 8-1-2015

**REVISED:** 

### 352AG3 Non-Employee Certification Administrative Guidelines

I HAVE READ AND UNDERSTOOD WCASD BOARD POLICY 352 ACCEPTABLE USE OF INTERNET, COMPUTERS, AND NETWORK RESOURCES AND AGREE TO ABIDE BY THIS POLICY.

Signature:
Date:
Complete the following:
Print name:
Non-WCASD Authorized Organization Affiliation:
Address:
Phone number:
Position or reason for needing network access/equipment:
School/building:
Time period using WCASD resources:
WCASD Administrator Signature:
Print name of WCASD Administrator:



Book Policy Manual

800 Operations

Title Employee Use of Personal Technology/Electronic Devices

Number 815.4

Status Active

Adopted August 1, 2015
Last Reviewed July 27, 2015

### <u>Purpose</u>

Section

In consideration of the recent proliferation and extensive utilization of personal technology devices, the district recognizes the need to establish guidelines for the use of such so as not to disrupt the primary function of the schools.

### **Definitions**

**Personal technology devices (personal technology)** shall be defined as any device capable of capturing, storing, and/or transmitting information, including text, audio, and/or video data, not owned by the district. These include, but are not limited to, such devices as:

- 1. Cellular telephones and smartphones.
- 2. Handheld, tablet, and laptop computers.
- 3. Digital music players, including without limitation iPods and MP3 players.
- 4. Digital and video cameras.

**Network** shall be defined as the group of interconnected computers systems, both wired and wireless, owned and used by the district in order to share analog and digital information, both voice and data, and access technology and the Internet.

### **Guidelines**

The district will monitor the use of all personal technology and, if connected to the network, monitor and log network utilization which may include deep packet inspection. The district reserves the right, in its sole discretion, to inspect, copy, store, remove, or otherwise alter any data, file, or system resources, encrypted or unencrypted, which may undermine authorized use of the network or the Internet.

In addition, the use of personal technology shall not violate local, state, or federal law, district policies including policies regarding Internet safety and acceptable use or discipline.[1][2]

### **Devices With Cellular or Satellite Connectivity**

1. Use of devices with cellular or satellite connectivity shall follow all district policies and shall not be used in a manner that causes a disruption of school activities. Incidental use for personal

communications is permitted; however, such personal use may not violate any district policies and procedures or interfere with job duties and performance.[1][2]

Personal technology that has the capability to take photographs or to record audio or video shall
not be used for such purposes while on district property or while an employee is engaged in
district-sponsored activities, unless expressly authorized in advance by the building principal or
his/her designee.

Devices Without Cellular or Satellite Connectivity Such as Laptop, Tablet, and Handheld Computers

Personal technology without cellular or satellite connectivity, such as laptop, tablet, and handheld computers brought to school shall be restricted to classroom or instructional-related activities. Personal technology can be connected to the district's network, including access to the Internet, under the following conditions:

- 1. The employee must follow the process defined by the Department of Technology for connecting personal technology to the district network and will not transfer or load the technology for use by another employee or student.
- 2. A Bring Your Own Technology Agreement must be filled out annually and returned to the Office of Technology prior to accessing the network or Internet. Personal technology discovered on the district network without a completed form may be confiscated by building administration or the Office of Technology.
- 3. The district retains the right to determine where and when personal technology may access the network. The district has preferred access to the network and all network devices.
- 4. As applicable, all personal technology should be running up-to-date virus detection software and operating system critical updates prior to accessing the network.
- 5. Software residing on personal technology must be personally owned or currently licensed. The employee must be able to provide evidence of proper licensing for all software installed on the personal technology when requested.
- 6. District-owned software or resources may not be installed on personal technology, unless designated by the Office of Technology, without written permission from the district.
- 7. Any software or application that degrades network performance, that consumes resources and/or bandwidth, or that is prohibited by district technology guidelines must not be used while connected to the network. This may include instant messaging, ISP clients, file sharing, streaming applications, and any software identified as a threat to district computer security.
- 8. Installation of a network device such as a personal wireless access point, router, hub or switch is prohibited.
- 9. Users may not create, implement or host their own servers or services while using personal technology at any time.
- 10. Users may not run software or take any actions that evade or interfere with the district's ability to monitor network use, scanning or reconnaissance or have the ability to hack into or in any way access private and/or confidential district or other third party resources or information.
- 11. File storage on the network or district-provided Internet resource is limited to schoolwork only.
- 12. The district is not responsible for providing or loaning any equipment, cabling, or software needed to connect to the network or technology resources. The district will provide no technical support for personal technology.

13. The Director of Information Technology, Superintendent, or his/her designee has the right to deny the connection of personal technology to the network. Personal technology may be removed from the district network at any time or for any reason on the recommendation of personnel listed above.

### **Delegation of Responsibility**

The district shall not be liable for the loss, damage, or misuse of any personal technology brought to school by an employee or to the inadvertent loss of data or interference with files for any reason.

The user of personal technology shall, at the discretion of the district, bear the costs of ensuring compliance with this policy.

Responsibility for the maintenance and repair of personal technology rests solely with the employee, except where specified in writing by the Office of Technology.

Violations of this policy by an employee may result in disciplinary action and confiscation and analysis of personal technology by school administration or his/her designee and/or transfer of personal technology to law enforcement agencies.[1]

The Office of Technology will promulgate procedures regarding the implementation of this policy. The district and school administration will support the expectations and responsibilities outlined in this policy and will work cooperatively with the Office of Technology to ensure network and data security.

Legal 1. Pol. 317

2. Pol. 352

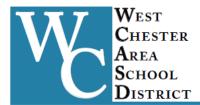
24 P.S. 510

Pol. 000

Pol. 717

Pol. 815.1

Pol. 815.2



782 Springdale Drive, Exton, Pennsylvania 19341 • Phone: 484-266-1000 • www.wcasd.net

### Retiree Substitute Volunteer Program (RSVP)

I have reviewed and understand the following West Chester Area School District's Board Policies:

- Policy 348-Unlawful Harassment
- Policy 352-Internet, Computers, and Network Resources Acceptable Use and Policy 352AG3-Non-Employee
   Acceptable Use of Internet Form (attached)
- Policy 851.4-Use of Personal Technology and Electronic Devices

I understand that the contents of these policies are my responsibility to abide by and follow as a participant in West Chester Area School District's Retiree Substitute Volunteer Program (RSVP).

Printed Name:	
Signature:	
Date:	

# WEST CHESTER AREA SCHOOL DISTRICT

ADMINISTRATIVE GUIDELINE

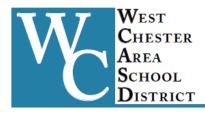
ADOPTED: 8-1-2015

**REVISED:** 

### 352AG3 Non-Employee Certification Administrative Guidelines

I HAVE READ AND UNDERSTOOD WCASD BOARD POLICY 352 ACCEPTABLE USE OF INTERNET, COMPUTERS, AND NETWORK RESOURCES AND AGREE TO ABIDE BY THIS POLICY.

Signature:
Date:
Complete the following:
Print name:
Non-WCASD Authorized Organization Affiliation:
Address:
Phone number:
Position or reason for needing network access/equipment:
School/building:
Time period using WCASD resources:
WCASD Administrator Signature:
Print name of WCASD Administrator:



782 Springdale Drive, Exton, Pennsylvania 19341 • Phone: 484-266-1000 • www.wcasd.net

## **Retiree Substitute Volunteer Program (RSVP)**

The West Chester Area School District offers a Senior Citizen Tax Rebate Community Service Program designed to assist Senior Citizens with the burden of Real Estate Taxes. Seniors may volunteer their services through the RSVP program. In return for their services, senior citizens may be entitled to a rebate of property taxes in accordance with the following guidelines.

### **Tax Credit Guidelines:**

- Open to Senior Citizens who are residents of the West Chester Area School District
- Minimum age limit to qualify for the tax rebate is 62 by December 31st of the year in which you are volunteering service.
- Tax rebates apply only to the property owned by the person volunteering service
- Property tax rebates will be made at the rate of \$8.00 per volunteered hour
- The maximum rebate allowed per household is \$560.00. This is based on 70 hours of volunteered service per household.
- Volunteers may opt to donate the credit to the School District (option on the application)
- Participants may volunteer in excess of 70 hours per year. However, the maximum real estate tax credit is \$560.00 or amount of property taxes, whichever is less. *Rebate amount cannot exceed actual amount of taxes paid.*

### **Business Office Procedures:**

- Volunteers must record their time on the monthly volunteer log (See Appendix Form H).
- A separate monthly volunteer log must be kept for each volunteer at each building location if duties are performed at more than one location.
- District Administrators must approve the monthly volunteer logs at the end of each month and forward them to the volunteer coordinator by the 3rd business day of the following month.
- Upon receipt of the monthly logs, the volunteer coordinator will enter the hours on a spreadsheet by volunteer name for tracking purposes.
- In January of each year, the volunteer coordinator will confirm with the volunteer the total number of hours of service for the year.
- No later than January 15th of each year, the volunteer coordinator will provide the real estate tax department with the list of volunteers from the previous year. The list will include the volunteers' name, home address, parcel number and number of hours of service volunteered for the year.
- The tax department will verify that the real estate tax bill for the volunteers' address was paid.
- After the tax payment has been verified, the tax department will issue a request for payment to the Accounts Payable Department.
- The Accounts Payable Department will process tax rebates by the end of February and mail them to the volunteer.

Appendix Form H

## RETIREE SUBSTITUTE VOLUNTEER PROGRAM - MONTHLY LOG

Month of \_\_\_\_\_\_, 20\_\_\_\_\_

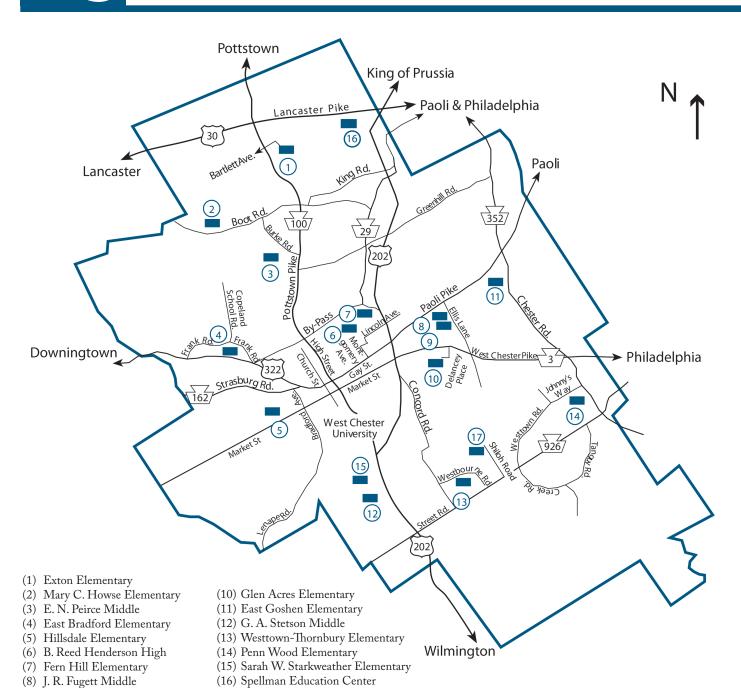
Date	Time In	Time Out	Total Hours	Date	Time In	Time Out	Total Hou
				-			
444	t the abov	e informat	ion is accurat				

# SITE MAP

(9) East High

West Chester Area School District, 782 Springdale Drive, Exton, PA 19341 Telephone: 484-266-1000 • Fax: 484-266-1175 • Website: www.wcasd.net

Facebook: facebook.com/WestChesterAreaSchoolDistrict Twitter: @WestChesterASD



(17) Bayard Rustin High