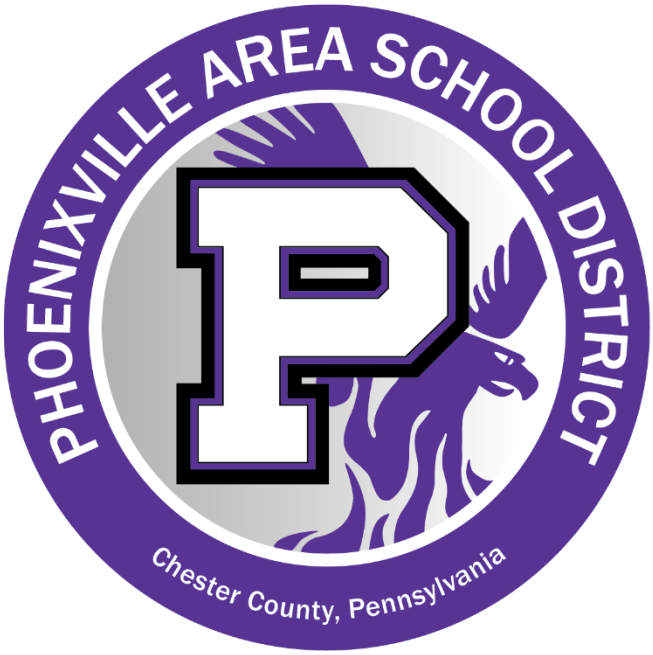
Phoenixville Area School District

(PASD)



2021-22

Technology for All

Guidelines for Students and Parents

Office of Technology
386 City Line Ave
Phoenixville, Pa.
19460

CONTENTS

PASD Virtual Program

In September PASD will be ensuring that students in K through 12th grade are equipped with a portable computer that the student will use at school and home throughout the school year. The computers the District provides are Windows-based and selected for their ease of use, portability, and durability. PASD will own non-BYOT (Bring Your Own Technology) computers and parents/legal guardians and students may share an annual cost for accidental damage coverage. Teachers receive ongoing professional development to identify and promote best practice teaching strategies in virtual classrooms. In many cases, students may keep their computers through the summer months. Our program has drawn upon and incorporated best practices of successful virtual programs from around the nation.

A. PRIMARY SCHOOL PROGRAM

Our primary program builds and reinforces basic computer skills for learning. Primary computer literacy classes play an important role in teaching students to become users and creators of technology rather than just consumers of technology. Primary school students will participate in an orientation program that will review Internet safety skills introduced in the elementary schools, as well as develop Internet research skills, copyright awareness, and best practice in the care of the device.

B. SECONDARY SCHOOL PROGRAM

Students in 8th grade and above will receive a new secondary computer that they will retain throughout their high school years. Freshmen will go through an orientation program addressing important issue in technology use, Internet safety, and academic research.

Important details governing the program are covered in this Handbook. Please take some time to review it carefully.

DEVICE PROTECTION PLAN (DPP)

Taking care of a computer can be a big responsibility, so we have put in place safeguards to protect the district's investment and to reassure parents/legal guardians and students. In turn, parents/legal guardians will participate in the DPP described below. An annual fee of $50 can be paid online or by cash or check at the Office of Technology. There is a $150 annual cap for each household.

While we expect students to take good care of their computers, accidents and malfunctions do occur. The district will provide a loaner computer to a student if their computer needs to be repaired or has been lost/stolen while the computer is being repaired or replaced.

A. WHAT IS THE DEVICE PROTECTION PLAN?

The Device Protection Plan is a $50 per student annual fee* that covers protection for your student's District Issued laptop computer during each academic year. The DPP provides 100% coverage for the first repair or replacement of the computer resulting from incidents such as accidental drops, liquid damage, and mechanical failures beyond the standard manufacturer's warranty that would otherwise be chargeable to the student and/or parent/legal guardian.

* There is a $150 annual cap on the cost of DPP for families with multiple student participants

B. WHAT DOES THE DEVICE PROTECTION PLAN COVER?

- Cracked Screen/Broken Cases
- Liquid Damage
- Trackpad/Keyboard
- Mechanical Failures not covered by the manufacturer's warranty

C. WHAT THE DEVICE PROTECTION PLAN DOES NOT COVER …

- Negligent** or Intentional*** damage
- Lost or Stolen devices
- Lost or damaged power cord and battery

**Negligent - failing to exercise the care expected of a reasonably prudent person in like circumstances
***Intentional – willful and/or deliberate

The determination of negligence will be made by school and district administrators and Dell. In case of vandalism by a person other than the student to whom the computer was issued, an investigation by the school administration and police will determine who is responsible for repair or replacement. In the event of three or more losses due to negligence or intentional damage, the district may restrict transport of the computer.

D. COVERAGE CONDITIONS

This DPP plan must be purchased by October 1st. Coverage provides for one incident per year. There is a $50 deductible for a second incident in that year and a $75 deductible for a third.

The cost of repair/replacement of damaged device beyond three per year will be the responsibility of the student and/or parent/legal guardian.

E. ACCESSORY REPLACEMENT

The student and parent/legal guardian will be responsible for the cost of replacing the items listed below.

a. Charger - $50

F. FINANCIAL HARDSHIP

If the DPP creates a financial hardship for a student and parent/legal guardian, please contact the school administration for information about scholarships and payment options. Students will still be responsible for repair and replacement costs due to negligence or intentional damage.

ONLY ONE USER

The computer is to be used only by the assigned student and should never be loaned to anyone else. The computer is registered to the student and the student alone is responsible for it. Parents/Legal Guardians may use the computer to monitor a student's classwork or use.

EXPECTATIONS FOR USE

A. RECEIVING THE COMPUTER

1. Students will receive their computers and cases in their schools at the beginning of the school year. Each device specifies the serial number and asset tag number of the computer assigned. Students should at that time ensure that the power supply and bag are present and inform a tech associate assigned to the school of any damage or defect.
2. Students should login before they leave the building so that the setup process can be completed. This will normally be done in a class or homeroom immediately following computer distribution.
3. Students and parents/legal guardians should review the Acceptable Use Policy and this Handbook to become familiar with expectations for use.
4. The district retains ownership of both the computer and installed software.

B. DAILY USE

1. Students are expected to bring a fully charged computer to school every day unless told otherwise by school administration, just as they are expected to bring their textbooks to school. Likewise, students are expected to take the computer home each night to complete assignments. Not taking the computer home will not be a valid excuse for an unfinished assignment.
2. Students are responsible for care both in and out of school.
3. Students may be subject to loss of privilege, disciplinary action, and/or legal action if they are found in violation of policies and guidelines found in this Handbook, the Student Handbook, and the district's Acceptable Use Policy.

C. CLASSROOM PROCEDURES

1. Each teacher will have rules and procedures related to the use of computers in their classroom. Students are expected to follow these computer rules just as any other classroom rules and a teacher can take disciplinary action as appropriate to maintain a safe and productive learning environment in the classroom.
2. One possible disadvantage to having a computer in class is that the computer can be a distraction. Students should remember that the computer is to be used for learning, not for playing games or surfing the Internet. Staying on task and focusing on the learning goal will make the best use of the technology. During the time spent playing games, students will be missing information that is important for their learning. Following the classroom "lids up/down" signal promptly will optimize the use of valuable learning time. The district reserves the right to impose access restrictions to the Internet if the computer becomes a distraction.
3. The teacher will not be responsible for teaching students every menu and command available in the various software programs. Students should familiarize themselves with the Help options in the program and on the Internet and exchange how-to information with peers so that they can efficiently create high-quality work.

REVIEW OF ACCEPTABLE USE AND OTHER POLICIES

In the virtual program a student has access to the network and the Internet throughout the school day, however, use of the computer and other technology resources is a privilege that rests on the responsible use of those resources. Guidelines for appropriate use are contained in Board policy 815 ("Acceptable Use Policy"). It is important that students understand and follow these guidelines which are summarized, in part, below for your convenience with the complete policy available through the district website. Any violations of these Guidelines may result in the loss of Internet privileges, appropriate legal action, and other disciplinary measures as described in Board policies related to student discipline and acceptable use of technology.

A. PERSONAL RESPONSIBILITY

It is the responsibility of users to learn about safe and appropriate use of the PASD network and Internet. This topic is covered throughout the K-12 library and technology curricula.

B. ACCEPTABLE/UNACCEPTABLE USE

1. Users are personally responsible for compliance with these requirements at all times when using the PASD network and Internet.
2. The following are examples of unacceptable uses. However, PASD may, at its sole discretion and at any time, deem other uses to be inappropriate uses of the network or Internet
   a. Using any material that is in violation of any United States legal code or any state legal code, including but not limited to copyrighted material;
   b. Using, sending, or supplying any material which is obscene, threatening, sexually explicit or in any way considered inappropriate in a school environment;
   c. Participating in any illegal activities of any kind;
   d. Using computer resources for hate mail, defamatory statements, statements intended to injure or humiliate others by disclosure of personal information (whether true or false);
   e. Sharing or using others' logons or passwords or other confidential information;
   f. Accessing another individual's materials, information, or files without permission;
   g. Circumventing or interfering with PASD Internet filtering obligations.

C. NETWORK AND INTERNET ETIQUETTE AND PRIVACY

All computers, network, and communications systems are the district's property and are to be used primarily for educational purposes. The district retains the right to access and review all electronic and voice mail, computer files, databases, and any other electronic transmissions contained in or used in conjunction with the district computer, network, and communications systems.

a. General etiquette rules:
   - Be polite
   - Never send or encourage others to send abusive messages
   - Use appropriate language. Remember that the user is a representative of their school. What is written can be viewed world-wide! Never swear, use offensive or obscene words, or any other inappropriate language.
   - Report messages relating to, or in support of, illegal activities to the building administrator or a teacher.
   - Do not disrupt the computer network in any way.

D. NETWORK ACCOUNTS

1. PASD has provided students with network accounts. The network accounts are intended to be used for academic purposes only and to be only used by authorized persons.
2. PASD has access to all network activity to ensure compliance with PASD policies. Users have no expectation of privacy in the system or any specific messages or materials.

E. SAFETY AND SECURITY

1. The user should never give out identifying information including last name, address, phone number or their photograph, social security number over the Internet and should never agree to meet in person anyone they have met online.
2. The user should never respond to items that are suggestive, obscene, harassing, demeaning, belligerent, or threatening.
3. The user shall notify an adult immediately if they receive a message that may be inappropriate or if they encounter any material that violates the Acceptable Use Policy.
4. While reasonable precautions will be taken to supervise student use of the Internet, PASD cannot reasonably prevent all inappropriate uses.

F. VANDALISM

1. Vandalism includes any attempt to harm or destroy the system, the hardware, the software, or the data of another user or any other agencies or networks that are connected to the Internet.
2. Any vandalism will result in the immediate loss of computer services, school disciplinary action, and a referral to appropriate law enforcement agencies.

COMPUTER CARE INSTRUCTIONS FOR STUDENTS

A. GENERAL PRECAUTIONS

1. Don't deface the computer, serial number or asset tag information. Do not remove or attempt to remove the district's identification labels from the computer. Do not write on, scratch, or otherwise deface the sticker or the outside of the computer.
2. Don't place any food or liquids next to the computer; never store food or drink in the computer case.
3. Do not leave the computer in any place where it might be stepped on or within reach of small children or pets.
4. Make sure your computer is used on a surface that allows adequate ventilation. Using the computer on a rug or in bed may cause it to overheat. In fact, we do not recommend using the computer in bed or just before bed time.
5. Don't expose or store your computer in extreme heat or cold. For example, don't leave your computer in a car for a long time during a hot summer or a cold winter day. Let your computer come to room temperature before you turn it on if it is warm or cold.
6. Conserve your battery. Put the computer into power-saving mode whenever possible to conserve battery life. Other ways to extend the battery life are to close the lid whenever possible and dim the screen brightness. Shut down the computer before closing it if you are not going to use it for a long time.
7. Take care inserting and removing cords and connections. Keep the computer cables away from magnets or magnetic fields which may include telephones/cell phones, speakers, and vacuum cleaners.
8. Always unplug and turn off the computer before cleaning. Clean the keyboard and touchpad with a cloth lightly dampened with water. Never spray a cleaner directly onto

the keyboard or computer. Do not power on the computer until all liquid has dried or been removed.

B. CARRYING COMPUTERS

1. Always transport the computer in the carrying case provided by the district. Note that the carrying case may be personalized to make it easy to distinguish from other students' cases.
2. To conserve the battery, be sure the computer is turned off and closed before placing in the carrying case if you do not intend to use it for a long time.
3. Never pick up or carry the computer by its screen.
4. Always close and disconnect all cords before carrying.
5. Use the case only to carry the computer and don't overload the case with books or sharp objects that can cause damage. Never put any bottle containing liquid in the carrying case.
6. You may put a dryer sheet in the case, especially during the winter, to reduce static electricity.

C. SCREEN CARE

Screens can cost over $300 to repair or replace, so you need to be sure to take special care to prevent damage.

1. Avoid touching screen with pencils, pens, or other sharp objects
2. One of the most common sources of screen damage is pressure placed on the top of the computer by books or other heavy objects, either in a backpack or on a hard surface. Don't stack anything heavy on top of the computer and be careful that the computer is on top rather than on the bottom when the backpack is set down.
3. Don't be rough when opening and closing the lid
4. Be sure there is nothing on the keyboard, such as pencils, pens, earphones, that can press against the screen when it is closed.
5. Never pick up or carry the computer by the screen
6. Clean the screen with lint-free, anti-static or microfiber cloth or wipes. Never use a liquid cleaner such as window or glass cleaner.

D. COMPUTERS LEFT UNSUPERVISED

1. The computer should never be left in unsupervised areas including the cafeteria, outdoor tables and benches, buses, locker rooms, classrooms, gyms, dressing rooms, restrooms, hallways.
2. The computer should be locked in a student's locker or a computer locker if they will be in an unsupervised area.
3. In case of a fire drill or other evacuation, follow the directions provided by your teacher.
4. Students should avoid taking or using their computers in an area where theft and damage are likely.
5. Computers are never to be used in locker rooms or rest rooms.

E. BASIC TROUBLESHOOTING

Don't panic—most computer problems can be fixed quickly. If you keep your files in your Office 365 drives, and/or have a backup, it is unlikely you will lose anything.

Computer isn't turning on:

- Check that your battery has enough power
- If your computer is plugged in, check that the power cable is plugged in securely. Only use the district provided power supply.

Cannot log into computer:

- The first time you log into the computer you must be at a district site.
- Check to make sure your Caps-Lock is not on
- Make sure there are no spaces in your username

Your device sees a Wi-Fi network but cannot connect to it:

PASD Student (district Wi-Fi):

- If others around you cannot connect it may be a problem with internet in the area.
- Try restarting the computer and see if it connects after a successful login

Wi-Fi networks outside the district:

- Make sure the password is entered correctly, most are case-sensitive.
- You may not have permission to access that network. There are many different ways to block access to a network and having the password may not be enough.
- If it is possible to do so, restart the Wi-Fi router.

Program is frozen or not responding:

- Write down what you were doing when the program froze or stopped responding.
- Restart the computer when the window or program will not close.

Receive an error message:

- Error messages give useful information about what went wrong. Write it down exactly as it appears. Different terms and numbers can mean different problems.

Restarting can fix many problems but has consequences:

- Always try to restart the computer by going to the start menu and clicking on restart.
- If this cannot be accomplished because the computer is completely frozen, a forced shutdown may be the only option. Hold the power button down until the computer shuts down. Wait about 30 seconds then turn the computer back on.
- Restarting the computer or forcing the computer to shutdown can result in lost data. You should only choose this option if no other options are available. It is good practice to save your work early and often.

If you are unable to resolve the problem, contact Technical Support as described below.

F. TECHNICAL SUPPORT

1. On-site help from the Technology Associate available during regular school hours for assistance with the following:
    a. Forgetting a password or being locked out of the network because of too many incorrect password attempts
    b. Cannot connect to the wireless network or frequently being dropped from the network
    c. Hardware issues such as inability to start up, hard drive access or crashes, or trackpad, keyboard, or mouse problems
    d. Software issues such as the need to be updated, program will not launch, or freezes repeatedly
2. Technical support procedure
    a. Bring the computer, carrying bag and charger to the Technology Associate after getting permission from your teacher to do so.
    b. If the Technology Associate is unable to fix the problem within a reasonable amount of time, the Technology Associate will keep the computer for repair and give the student a loaner computer, if there is one available, until the computer is repaired.
    c. If the repair involves a hard drive or any files on the hard drive, the hard drive will be erased and returned to the original state. Note that any personal files or software on the computer cannot be restored. It is important to keep important files in the Office 365 drives.
    d. Only authorized district personnel may facilitate repair of a district-owned computer. Students should not attempt to repair or allow anyone other than authorized district personnel to attempt a repair of the computer.

USING THE COMPUTER AT SCHOOL

A. POWER MANAGEMENT

1. Bring your computer to school every day, fully charged unless told otherwise by school administrators or teachers. An otherwise functional computer with a dead battery is no excuse for late or missing work or the inability to participate in a class activity.
2. Be careful of the tripping hazard posed by a power cord if the computer must be plugged in to charge it in a classroom or library.
3. A fully charged computer used judiciously for classroom work should get you through the day without needing to plug it in.

B. SOUND/EARPHONES

1. Mute the computer sound at all times unless given explicit permission by a teacher to use the sound for educational purposes.
2. Earphones or ear buds may be used at the discretion of an individual teacher.

C. CAMERA

1. The built-in camera is to be used for educational purposes only. Any use that violates the privacy rights of others will be subject to disciplinary action.

2. Ask the person's permission before you take, post/share a photo with others. Remember that photos that start off as a joke can escalate into cyberbullying and humiliation for someone else, especially if the photo is in any way unflattering, embarrassing, or compromising.
3. Although the district cannot and will not access the built-in camera for monitoring purposes, if you are uncomfortable with the camera you may cover the lens with a piece of paper. Do not apply tape directly to the lens since that will cause damage and make it unusable.

D. MANAGING FILES

1. No apps, folders, or files loaded on the computer by the district should be deleted or altered in any way. Do not install any software or games other than what the district licenses and distributes through the district software center.
2. You should save your school work to your Office 365 drive. The district is not responsible for files that are lost on a hard drive or flash key.
3. The computer's hard drive may be reimaged at the end of a year or as a result of a repair, so be aware that any files or programs stored on the hard drive will be erased.

E. INTERNET FILTERING

The Children's Internet Protection Act (CIPA) enacted by Congress in 2000 and updated in 2011 requires that schools and libraries that receive federal e-rate discounts must implement technology that blocks access to pictures and other content that are (1) obscene; (2) child pornography; or (3) harmful to minors. Internet safety information is also presented to students at each school as part of CIPA regulations. More information about this Act can be found at http://www.fcc.gov/guides/childrens-internet-protection-act. No web filter is 100% reliable, however, and students should immediately report any display of inappropriate material to their teachers or administrators.

The District Laptop comes with installed Internet filtering software installed.

1. Printers will be available at various locations around the school. You will receive instructions from your teachers about how to add a printer to your computer.
2. Printing is limited to only those items needed directly for instruction.
3. Turn in as many assignments electronically as possible either by uploading to Canvas, an Office 365 Drive shared folder or by emailing your teacher, based on teacher direction.

F. ATHLETIC PRACTICES AND FIELD TRIPS

1. Do not bring your computer to athletic practices, games or other events which include the bleachers, a bus, or the sidelines.
2. Computers are not allowed on overnight trips or field trips without written approval of a teacher, administrator, or parent/legal guardian.
3. Don't store your computer in an athletic locker.
4. The coach has the discretion to ask students to bring their computers to an athletic event for the purpose of instruction. In this situation, the coach will make arrangements for safe use and storage of the computers when they are not in possession of the students.

G. HARDWARE

1. Under no circumstances should anyone other than authorized district personnel repair or reconfigure the laptop computer. No attempt should be made to open or alter the internal components of the computer. Removing any screws will render the warranty null and void.
2. Installation of internal hardware is strictly forbidden.
3. No network hardware or software that sets the computer as host or component of a peer-to-peer network is permitted.

H. INSPECTION/PRIVACY

There is no expectation of confidentiality or privacy. Computers may be inspected at any time when there is a reason to believe that district rules have been violated. The district retains the right to access and review all electronic transmissions and transmission logs contained in or used in conjunction with the district's computer system and electronic mail system.

USING THE COMPUTER AT HOME

A. INTERNET ACCESS

1. The district will provide information and share tips for how to connect your computer to your home network, but you may be required to contact your Internet Service Provider to troubleshoot the connection. The district can give only very limited support for home network connections because of the wide range of providers and home setups.
2. The district has installed a web filtering application on the computer. However, parents/legal guardians may set appropriate parental controls on their home Internet connection, as long as it does not interfere with the functionality of the installed filtering software, and parents should supervise their child's use of the Internet to ensure safe and appropriate Internet use. Parents/Legal Guardians should set expectations for appropriate content, music and videos. If inappropriate content is found downloaded onto the computer, the student will be in violation of district policies and may be disciplined.
3. We are aware that not all families have Internet access in their homes and teachers will keep that in mind when they make assignments. Students who don't have home Internet access will be able to download most assignments or can use public places with

Wi-Fi, such as the library and some restaurants if they need to work on the Internet. Low cost Internet options include Comcast that offers $10/month Internet access for new customers and Verizon that offers a $20/month DSL connection. Students are also encouraged to purchase a flash drive on which to store information to work on at home.

4. Students should not "borrow" someone else's Internet access, be it a neighbor or any other private Internet connection. Such Internet use is illegal and offenders can be fined and/or jailed for using an access point without the owner's permission. Please let your school know if home Internet access is a challenge. There may be ways we can assist.

B. HOME PRINTING

Since there are thousands of different printer models, we cannot guarantee that the computer will be able to connect to a home printer. However, the Windows Operating System is widely used in both home and enterprise environments. It would be unlikely that connectivity to a printer will be a problem.

C. SURGE PROTECTOR

1. Use a surge protector when you plug in your computer at home to protect against power fluctuations that can damage your computer or its battery.

LEAVING THE DISTRICT

If you move or leave the district to go to another school, you must return the computer on your last day in the district. The computer and charging cord should be taken to the Technology Associate and the computer will be powered on so that it can be checked for damage.

If you leave the district and do not return the computer, the district will make a reasonable attempt to recover the computer. If the attempt is unsuccessful, after one week the district will treat the computer as stolen and notify the appropriate authorities.

SOFTWARE

A. DISTRICT SOFTWARE

1. Do not change computer name
2. Do not change operating system extensions
3. No apps, folders, or files loaded on the computer by the district should be deleted or altered in any way.
4. Software and operating system updates will be applied to the computer automatically when you log into the district network. You should allow the updates to be completely installed so as not to endanger network security or interfere with applications that may be needed for assignments.
5. Do not copy or distribute in any way district-owned software

B. VIRUS AND MALWARE PROTECTION

District-purchased virus and malware protection software is installed and should not be deleted and/or altered in any way. This software is regularly updated when the computer is on the district network.

C. PERSONAL SOFTWARE

1. Personal software may not be installed on the computer and will be deleted when detected. Music, games or any other application that interferes with the use of the computer in school is prohibited.
2. Students should become familiar with the copyright regulations and understand the limitations of "fair use" when downloading and/or using materials such as photos, music, or videos from the Internet. Copyrights are implicit, and there does not have to be a copyright notice for the material to be protected. Also, some photos have restrictions placed on them. Properly crediting the source of materials is the best approach to demonstrating good research practice.

REPORTING THEFT AND VANDALISM

Students should keep in a safe location a record of the make, model, and serial number of their computer that can be referred to in the event of theft of the computer. A form is located at the end of this Handbook on which to enter this information.

Theft of the computer while at school or on district property must be reported immediately to a teacher or administrator. The student and parent/legal guardian must cooperate fully with school officials and police officers in the investigation of the theft.

Theft of the computer outside of the district must be reported both to the school administration and to the appropriate Police Department. A copy of the police report must be submitted to the school administration within five days along with the following information: date and address of theft, detailed description of theft, police file number, officer's name and police agency contact information.

BRING YOUR OWN TECHNOLOGY (BYOT)

While we plan to provide a computer to each student, a student and their parent/legal guardian may prefer for the student to bring a personally-owned computer from home instead of using a district computer and may access a designated wireless district network. Please know that we will not be able to install district-licensed software on a student- owned computer and there will be limited district support. There is no charge for the BYOT program and the procedures, FAQs, and forms can be found on the district website under Departments, Technology, Bring Your Own Technology.

Students bringing in their own computers are still accountable for their use and must follow the Acceptable Use Policy. Most of the considerations and care of the computer listed in this Handbook may also apply to BYOT and are recognized as good computing habits. The district

assumes no responsibility for mishaps while transporting or using a personally owned device for school and on the district's network.

FOR PARENTS/LEGAL GUARDIANS

We know that parents/legal guardians may be apprehensive with the thought of their child being responsible for a computer in and out of school. Typically damage and theft are the biggest worries which are why we purchase the warranty and accidental damage coverage.

While students are responsible for the computer, we recommend that parent/legal guardians take an active role in their child's learning and how they are using the computer at home and school. Parents/Legal Guardians are asked to familiarize themselves with this Handbook and monitor their child's use to ensure proper care and safety. Every family has different rules related to where and how a computer may be used at home, and we encourage you to have on-going discussions with your children about your expectations. Especially learn about social networking applications such as Twitter, Snap Chat, and Instagram and guide your child in what is appropriate to share with others. The district provides a comprehensive collection of resources for parents on the district website.

Review the Acceptable Use Policy with your child to be sure that they understands the scope of, and consequences for not following the Guidelines. If you are a proficient technology user, model good use of computers for writing and completing work assignments for your child and provide hints on saving and organizing work.

Children can become engrossed in their online activities, therefore, be sure that your child takes frequent breaks from using the computer and engages in healthy physical activity. Tasks such as typing or using the trackpad can cause repetitive strain injuries that can have long-term consequences. Eyestrain and neck strain can also be aggravated by the lengthy intense use of the computer. Again, we do not recommend computer use in bed or just before bedtime, as backlighting may interfere with the ability to fall asleep.

We believe that students can use the computer responsibly, but we know from experience that lapses of judgment do happen and you may be required to reimburse the district for damages or loss. We know that in such a situation you may feel stressed or upset but please be respectful when communicating with the Office of Technology as they are only trying to protect the district's investment in the program and ensure its continued success. We will always do our best to work with you in balancing the protection of the district's investment with individual family circumstances and we will not deny student access to academic resources based on ability to pay. We may, however, exercise options permissible under Board policy and PA School Code to collect money owed to the district.

QUESTIONS AND CONCERNS

For any other questions or concerns you have about the program please contact the Office of Technology:

Web: https://www.pasd.com/departments/technology/resources

Telephone: 484-927-5098

DEVICE IDENTIFICATION FORM

DEVICE IDENTIFICATION INFORMATION

Computer manufacturer _____

Computer model _____

Serial Number/Service Tag _____

Please keep this information in a safe place separate from the computer.

Digital Technology and Acceptable Use

Code

815 AR

Status

Active

Last Revised

September 17, 2015

ADMINISTRATIVE
GUIDELINES POLICY NO.
815
DIGITAL TECHNOLOGY AND ACCEPTABLE
USE

Prohibitions – Students And Employees

Students and employees of the District shall not:

1. Use any DIGITAL TECHNOLOGY for any purpose other than for the legitimate educational purposes of our students or for purposes of advancing the legitimate business of the District.
2. Use any DIGITAL TECHNOLGY for personal business or affairs, except as expressly provided in this policy or in administrative guidelines promulgated and adopted by the SUPERINTENDENT.
3. Use any District COMPUTERS or DATA unless and until a confidential USER ID and password has been assigned to the student or employee.
4. Use any District COMPUTERS or DATA without using USER ID and password.
5. Terminate use of any COMPUTERS without logging off the COMPUTER.
6. Disclose USER ID or password to any other individual.

7. Open or log on to any COMPUTER, software, program or application using, utilizing or inputting the USER ID and/or PASSWORD of any other individual or entity, or use any default or preset USER ID and/or PASSWORD without express authority of the Superintendent or designee.
8. Misrepresent identity when using the District's COMPUTERS.
9. Bypass any blocking or security software that may be used or installed by the District.

17 U.S.C. Sec. 101 et seq Pol. 814	10. Intentionally, willfully, maliciously or through reckless indifference damage or corrupt the functioning of any DIGITAL TECHNOLOGY or any data stored, either temporarily or permanently on any DIGITAL TECHNOLOGY. 11. Visit or access pornographic websites. 12. When using the District's DIGITAL TECHNOLOGY, violate the District's Code of Student Conduct or any other applicable policy of the District. 13. Use any COMPUTERS unless and until the individual has signed an acknowledgment in the form prescribed by the District attesting to the individual's understanding of the rules governing the use of DIGITAL TECHNOLOGY. 14. Take possession of any COMPUTER unless or until the individual has signed an agreement in the form prescribed by the District setting forth the terms and conditions under which the individual is permitted and authorized to have possession of the COMPUTER. 15. Intentionally enter or hack into any secure or confidential area of the District's systems, network(s) or COMPUTERS without proper authority. 16. Violate any copyright laws or the ownership or license rights of any person or entity. 17. Violate the terms or conditions of any license owned by the District. 18. Violate the legal rights of others.

	19. Knowingly or willfully infect any COMPUTER with any virus. 20. Use any software or Internet site in violation of any applicable licensing agreement or applicable terms of use. 21. Use any DIGITAL TECHNOLOGY to gain unauthorized access into anyone else's COMPUTERS or networks in any way or manner that is not authorized. 22. Use any data mining, bots, or similar data gathering and extraction methods in violation of any person's or entity's rights. 23. Install any software program on or in or download any software program onto or in any COMPUTERS without the express written approval of the SUPERINTENDENT or designee, except for the following:

	a. Printer drivers. b. Adobe® Acrobat® Reader®. 24. Fail to report to the District's technology director any time when s/he inadvertently visits or accesses a pornographic site. 25. Violate any applicable work rule when using the District's DIGITAL TECHNOLOGY. 26. Alter or change the look or operation of any COMPUTER. 27. Delete or remove any program, application, security feature, or virus protection from any District COMPUTER. 28. Incur any charges or costs of any nature or type to the District in connection with DIGITAL TECHNOLOGY or use of DIGITAL TECHNOLOGY; except as specifically and expressly authorized in accordance with applicable procurement requirements established by the District or by law, or telephone charges by an employee incurred for District purposes and consistent with the employee's authority. 29. Enter or use a COMPUTER or DATA or SYSTEM in an unauthorized manner.

	30. Plant any virus, pornography or other prohibited content or software on any COMPUTER. 31. Disconnect any computer from the network without prior explicit direction to do so, except for laptop computers issued with the expectation that they will be disconnected from the network. 32. Disconnect any hardware from any computer without prior explicit direction to do so, except with respect to laptop computers issued with the expectation that they will have hardware, such as printers, connected and disconnected. 33. Access another's COMPUTER for any improper or unlawful purpose, INCLUDING to activate the audio or video functions of the COMPUTER or to search the COMPUTER'S files, documents or codes, without the person's prior permission and authority or take control of in any manner. 1. Integration into Curriculum and School Program. The SUPERINTENDENT or designee shall promulgate and adopt appropriate administrative guidelines governing how DIGITAL TECHNOLOGY will be integrated into the curriculum and school program.

47 U.S.C. Sec. 254 SC 1303.1-A Pol. 249	2. Training Students and Employees. The SUPERINTENDENT or designee shall appropriately train students and employees with respect to the permissible uses of DIGITAL TECHNOLOGY. 3. Phoenixville Area School District provides instruction to minors on the topics of Internet safety and appropriate online behavior. Internet safety education topics include, but are not limited to: online behavior and ethics, social networking safety, chat room safety, cyberbullying awareness and response and other online privacy and security issues. 4. Code of Student Conduct. The SUPERINTENDENT shall cause the Code of Student Conduct to be amended as appropriate to reflect the applicable terms and conditions of this policy.

Pol. 815.2	5. Updating/Upgrading DIGITAL TECHNOLOGY. The SUPERINTENDENT or designee shall promulgate and adopt appropriate administrative guidelines to ensure that DIGITAL TECHNOLOGY is updated and upgraded in a systematic and cost effective manner. 6. Access To and Safekeeping of DIGITAL TECHNLOGY. The SUPERINTENDENT or designee shall promulgate and adopt appropriate administrative guidelines governing who will be provided with DIGITAL TECHNOLOGY; how DIGITAL TECHNOLOGY will be provided to students and employees; and how DIGITAL TECHNOLOGY will be properly safeguarded. 7. Enforcement of Policy and Guidelines. The SUPERINTENDENT shall promulgate and adopt appropriate administrative guidelines for the enforcement of this policy and the guidelines adopted in accordance with this policy. Each student and employee using the District's TECHNOLOGY shall execute an acknowledgment that s/he has received a copy of this policy and understands that s/he is required to comply with its conditions. In the case of younger students, the SUPERINTENDENT shall administratively determine whether the acknowledgment should be signed by one (1) or more parents/guardians in lieu of an acknowledgment by the student. 8. District Website. The SUPERINTENDENT shall develop policy and/or administrative guidelines detailing the content of the District's website and the links that are placed on the website. <u>Privacy And Ownership</u> No employee or student using the District's DIGITAL TECHNOLOGY shall have any right of privacy or expectation of privacy with respect to anything done on or with said DIGITAL TECHNOLOGY; except with regard to the limitations

	respecting remote access of laptops. The DIGITAL TECHNOLOGY that belongs to, is licensed to, or is accessible through DIGITAL TECHNOLOGY is owned by or licensed to the District. The District retains all rights as an owner or licensee with respect to all DIGITAL TECHNOLOGY that it owns or licenses and has, unless restricted by an express agreement with a third party supplier, the rights of an owner or licensee, INCLUDING, the rights to use, transfer, inspect, look in, read, and/or store any such DIGITAL TECHNOLOGY. The SUPERINTENDENT shall develop administrative guidelines pertaining to the review of emails to or from students, parents or employees to ensure compliance with this policy. Notwithstanding anything herein to the contrary, no employee shall read or examine emails of Board members except: when necessary to comply with or respond to a public records request, a litigation hold requirement, or an order or subpoena in connection with an administrative or judicial action; or after written notice has been provided to the Board member that their email will be reviewed. The District owns all intellectual property rights of all work prepared or created by any employee in the course and scope of employment for the District, INCLUDING copyright, in accordance with the terms, conditions and limitations of applicable law. Consequently, no student, employee or visitor may violate the copyright or other intellectual property rights of the District or deprive by any means or manner the District's rights with respect to such material. <u>Permissible And Impermissible Uses Of DIGITAL TECHNOLOGY</u> *Students –* DIGITAL TECHNOLOGY may be used only for legitimate educational purposes and in a manner that complies with all rules and prohibitions contained in this policy or in other applicable policies.

	DIGITAL TECHNOLOGY is being provided or made available to students solely as part of the educational program; for the purpose of teaching students how to use and employ DIGITAL TECHNOLOGY; and to further the teaching of the District's curriculum and educational programs. The District is not, through DIGITAL TECHNOLOGY that is being made available by the District to students, creating a public forum, an open public forum or a limited public forum. DIGITAL TECHNOLOGY may not be used by students for speech or expressive conduct:

	1. That materially and substantially interferes with the education process. 2. That threatens immediate harm to the welfare of the school community, or to any individual. 3. That is lewd, vulgar, indecent or obscene or which contains sexual innuendo, metaphor or simile. 4. That encourages unlawful activity. 5. That interferes with another individual's rights. 6. That violates any applicable policy of the District. 7. That constitutes libel, slander or defamation. 8. That is sexually, racially or ethnically related, that is offensive, threatening or an affront to the sensibilities of others, and that is unlawful under the standards of the anti-discrimination laws of the United States.
Pol. 103, 248	All expressive conduct or material – whether verbal, written, or graphic – created, downloaded, maintained, copied, pasted, harvested or otherwise obtained, used or transmitted by, to, from or with the District's DIGITAL TECHNOLOGY, is required to be related to the adopted curriculum, assigned classroom activities, or school programs, such as the development of writing skills, the learning of legal, moral and ethical restrictions imposed upon speech and the acceptance of criticism.

	Consequently, all expressive conduct by students shall be: age-appropriate; consistent with the rules of grammar, spelling, sentence structure and format being taught by the District; and consistent with the abilities of the student. Students shall not use DIGITAL TECHNOLOGY provided by the District for any purpose not connected with the educational program of the District. This prohibition INCLUDES: any of the prohibitions set forth in this policy or in the Code of Student Conduct; gambling; accessing social network sites unless such access is specifically in accordance with a District assignment; and accessing any site for the purpose of defeating any of the prohibitions in this policy. *Employees –* The components of the District's DIGITAL TECHNOLOGY may only be used in a way which is consistent with the intended purpose of the DIGITAL TECHNOLOGY. DIGITAL TECHNOLOGY may only be used to further the curriculum or programs of the District.

Notwithstanding anything herein to the contrary, during such times as the employee has no work duties, the employee may use DIGITAL TECHNOLOGY to access his/her private or personal email account from which email may be sent or received through that account and not through any such an account of the District. No employee shall violate any of the provisions of this policy or of applicable law when accessing his/her private email account either during the work day or through the District's DIGITAL TECHNOLOGY. Any email account provided by the District shall be used only for advancing the interests of the curriculum or school programs, activities or functions.

Communication by employees reflects on the District. Consequently, expressive activity through DIGITAL TECHNOLOGY shall exhibit good grammar, proper style, and good spelling.

No program, software, application or patch may be installed or placed in any District COMPUTER that is not licensed to and in the name of the District or that is not authorized in writing to be installed or placed in any District COMPUTER.

Employees shall not use DIGITAL TECHNOLOGY provided by the District for any purpose not connected with the educational program of the District. This prohibition INCLUDES: any of the prohibitions set forth in this policy or in any other applicable policy or administrative guidelines of the District; gambling; accessing social network sites unless such access is specifically in accordance with a District assignment; and accessing any site for the purpose of defeating any of the prohibitions in this policy.

Employees shall not save or store any records, material, data, documents or files on any digital technology that does not belong to the District or that is not licensed to the District. Employees using digital technology to create, save or store student or District DATA must create, save or store such DATA on District DIGITAL TECHNOLOGY.

Employees shall not cause email to be diverted to or intercepted from the District's email system to an email or technology system not belonging to or licensed by the District.

Unless an employee has granted consent otherwise, the e-mail of the employee may not be automatically intercepted and redirected to another employee or person.

Special Rules Pertaining To Laptops Given To Students Or Employees To Take Home

In addition to all of the rules set forth in this policy or the Code of Student Conduct:

1. The Superintendent shall provide notification to PARENTS and students as to the students eligible to be issued a laptop.

Pol. 226

2. As a condition of the receipt of the laptop, both the student and the PARENT must sign an agreement in a form created by the District setting forth the obligations of the student and PARENT with regard to the care, use and possession of the laptop.
3. No employee or other person shall remotely access a student's laptop except for the following purposes and subject to the following terms and conditions exclusively:
   a. Resolution of Technical Problem. In some instances, it may be necessary for a technology employee to access the laptop remotely to resolve a technical problem. If this is needed, the student's or PARENT'S permission must be obtained before remote access is effectuated and must be properly documented. If permission for remote access is given, a permanent record of the approval must be logged, setting forth pertinent information, INCLUDING: the time, date, duration of remote access, and reason for remote access.
   b. Remote Software Maintenance. **Remote software maintenance** means the automatic downloading and configuration changes of software or settings when a student or employee connects to the District's network. This is permitted without obtaining any additional permission from a student, employee or PARENT.
   c. Voluntary Participation in Web-conferences or Other Web-based Activities. Participation in a web-conference or other web-based activity shall constitute the participant's agreement to access to the participant's COMPUTER and all components of same for all incidents associated with the conference or activity. No person engaging in such activity shall perform any function or activity not fairly or properly associated with the conference or web-based activity.

	d. Remote Search of Files, Documents, Pictures, Videos, Code or Software on Laptop. No employee or other person may search a laptop remotely unless: a remote search is reasonably necessary; the person is specifically authorized to conduct such a search; and the person has a reasonable suspicion that the student or employee is violating applicable laws or policies or rules and that evidence of same can be found on the COMPUTER or that the COMPUTER contains contraban This does NOT include district use of anti-virus oranti-malware software that remotely access the COMPUTER for the purposes of seeking and removing viruses or files harmful to the normal operation of the computer, or is in violation of any other part of this policy.

	Where such reasonable suspicion exists, the scope of the search must be reasonably related to the violations that justified the search. e. Video and Audio. No person may activate the audio or video functions of a laptop remotely at any time unless: 1. The functions are part of an online class or assignment. 2. After a laptop is reported lost or stolen in writing on a form developed by the District for this purpose by the employee or student to whom the COMPUTER has been issued. <u>Provision Of DIGITAL TECHNOLOGY Services</u> Students, in accordance with the programs in which they are enrolled, shall be provided with only the following DIGITAL TECHNOLOGY services: 1. Access to the Internet, subject to the policies, limitations, exclusions and conditions established by the District and applicable laws and statutes.

	2. Access to software as provided from time-to-time by the District and subject to the policies, limitations, exclusions and conditions established by the District. 3. Digital File Space from which to access or save work, which shall be subject to the policies, limitations, exclusions and conditions established by the District. 4. Print services, subject to the policies, limitations, exclusions and conditions established by the District. Employees, as designated by the SUPERINTENDENT, shall be provided with only the following DIGITAL TECHNOLOGY services: 1. Access to the Internet, subject to the policies, limitations, exclusions and conditions established by the District. 2. Email, subject to the policies, limitations, exclusions and conditions established by the District. 3. Access to software as provided from time-to-time by the District and subject to the policies, limitations, exclusions and conditions established by the District. 4. Digital File Space from which to access or save work, which shall be subject to the policies, limitations, exclusions and conditions established by the District.

	5. Print Services, subject to the policies, limitations, exclusions and conditions established by the District. Visitors. To visitors who may access the District's wireless networks in accordance with the terms, conditions and limitations of this policy and applicable administrative guidelines. Visitors shall not have any other access to District digital technology. Any such visitor must accept and agree upon all terms and conditions of use as set forth in the policy, administrative guidelines and/or agreement.

	No digital services shall be provided by the District to other individuals or outside companies, entities or suppliers. Disclaimer Of Liability/Disclaimer Of Warranties The District disclaims all liability and warranties, INCLUDING as follows: 1. There are no warranties, express or implied, by operation of law or otherwise, regarding or relating to the DIGITAL TECHNOLOGY provided by the District to any student, employee, visitor or other person or entity. The District specifically disclaims all implied warranties, INCLUDING those of merchantability and fitness for a particular purpose. 2. No representations or other affirmation of fact, INCLUDING to statements regarding capacity, suitability for use, or performance shall be deemed to be a warranty by the District for any purpose or give rise to any liability of the District whatsoever. 3. The District shall not be liable for any lost or stolen digital or electronic data, files, documents, or material of any kind that any student, employee or visitor prepares, creates, stores on, sends to, saves to, copies to, or otherwise uses in connection with the District's DIGITAL TECHNOLOGY or any component thereof. Discipline
Pol. 218, 233, 317	Students and employees shall be subject to appropriate discipline, including dismissal in the case of employees, and permanent expulsion in the case of students, in the event that any one (1) or more provisions of this policy are violated. Complaint Procedure
Pol. 103, 103.1, 104, 248, 249 348, 906	If any employee, student, or other person has any complaint of any nature or type pertaining to DIGITAL TECHNOLOGY, the uses of DIGITAL TECHNOLOGY at the District or on its web site, INCLUDING complaints or concerns about sexual harassment (*see also*, District's Sexual Harassment Policy), bullying, cyber-bullying

Pol. 818	(*see also,* District's Bullying Policy and Code of Student Conduct), racial intimidation, discrimination, or ethnic intimidation, a complaint may be filed with the SUPERINTENDENT, who shall promptly cause the complaint to be properly investigated with the advice or assistance of the solicitor. <u>DIGITAL TECHNOLOGY Personnel</u> The District may, from time to time, employ individuals to create, set up and/or maintain one (1) or more forms of DIGITAL TECHNOLOGY. These individuals may be employees of the District or independent contractors retained for discrete services. All contracts with independent contractors must be reviewed by and approved by the solicitor and Board. DIGITAL TECHNOLOGY personnel, whether employed solely to create, set up or maintain DIGITAL TECHNOLOGY or employed to create or maintain DIGITAL TECHNOLOGY as an adjunct to other duties: 1. Shall execute an appropriate non-compete and confidentiality agreement, as developed by the solicitor, so that the individual: does not compete with the District in the use, sale or distribution of any DIGITAL TECHNOLOGY which the employee was involved in creating or developing for the District; does not disclose any confidential information; and does not use any confidential information for his/her personal benefit. 2. Shall not access any document, data, file or information stored in or accessible through the District's DIGITAL TECHNOLOGY unless access to such document, data, file or information is necessary for the individual employee to perform his/her duties as set forth in his/her written job description or to create or maintain any DIGITAL TECHNOLOGY in accordance with his/her written job description. Notwithstanding anything in this policy to the contrary, DIGITAL TECHNOLOGY personnel shall have such authority as is necessary to enable each to perform his/her specific job duties as set forth in writing in his/her job description.

	The SUPERINTENDENT shall review the job description of the head of the District's technology department no less frequently than annually and shall make such changes or adjustments to the job description as may be necessary or desirable. Provision Of Technology Or Services Nothing in this policy shall be construed nor is intended to prohibit the District from providing DIGITAL TECHNOLOGY or services related to DIGITAL TECHNOLOGY to others pursuant to contracts or other arrangements.