West Chester Area School District (WCASD)

2020-21 1:1 Guidelines for Students and Parents

Office of Technology
782 Springdale Drive
Exton, PA 19341
484-266-1050
one2one@wcasd.net

CONTENTS

WHY HAVE A 1:1 COMPUTER PROGRAM?

In a 1:1 or 1-to-1 computer program each student has a personal and portable computer available 24/7, to use in every class, in study halls, and at home. This practice is widely known as "anytime, anywhere" learning with the emphasis being on the transcending of the school walls. This is why we now refer to our 1:1 program as *World Wide West Chester*. When every student has a computer, teaching and learning can become much more dynamic and engaging which leads to deeper understanding and more connections to real world applications. Students can collaborate online with their peers in the class, in other schools, or in other countries to gain and contribute multiple perspectives. They can use their computers to research, gather, and evaluate information, write summaries, analyses, and opinions, and communicate effectively to convey meaning and rationale. While in class students may use their computers to take notes, do research, write assignments, complete an online quiz, create a multimedia presentation, or collaboratively create a shared document. In their classes, students will become proficient using software tools such as Microsoft Office and GoogleDocs—tools that are used in higher education and careers in the corporate world.

There is a collection of research on 1:1 programs that demonstrates many positive impacts on student learning resulting from changes in instructional practices and daily use of technology. When a 1:1 program is implemented effectively by teachers, students show increased student engagement, decreased dropout rates, and gains in student achievement. The instruction is more student-centered through increased incorporation of authentic and hands-on activities. Feedback from WCASD students who participated in pilot 1:1 programs showed that students were taking more responsibility for their learning, an important skill that will become essential as more classes and textbooks move to an online venue. The research confirms that technology by itself cannot improve test scores. But technology can help transform teaching practices to make learning more meaningful, relevant, and permanent.

The West Chester Area School District recognizes the importance of providing a technology-rich learning environment to prepare its students for maximum success as they continue their education or enter the workforce and the 1:1 program is an important tool to take students to the next level of achievement.

THE WORLD WIDE WEST CHESTER 1:1 PROGRAM

In September WCASD will be giving each participating student in 6 through 12th grade a portable computer in a carrying case that the student will use at school and home throughout the school year. The computers are Windows-based and selected for their ease of use, portability, and durability which students indicated were important factors. WCASD will own the 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 1:1 classrooms. In most cases, students may keep their computers through the summer months. Our program has drawn upon and incorporated best practices of successful 1:1 programs from around the nation.

A. MIDDLE SCHOOL PROGRAM

Our middle level 1:1 program builds and reinforces basic computer skills for learning. Middle school computer literacy classes play an important role in teaching students to become users and creators of technology rather than just consumers of technology. Middle 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. Students will keep their device through 8th grade.

B. HIGH SCHOOL PROGRAM

Students in 9th grade will receive a new 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 1:1 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 for a teenager, so we have put in place safeguards to protect the district's investment and to reassure parents/legal guardians and students. In turn, we ask that parents/legal guardians to consider participating in the DPP described below. An annual fee of $50 can be paid online using the PaySchools system or by cash or check at the Office of Technology. The benefits could pay for themselves with one mishap. Parents or guardians who do not opt to participate in the DPP may be liable for the full cost of a repair or replacement resulting from accidental damage.

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 1:1 laptop computer during each academic year. The DPP provides 100% coverage for the 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 failure resulting from a covered event

C. WHAT THE DEVICE PROTECTION PLAN DOES NOT COVER ...

- Negligent** or Intentional*** damage or theft resulting from negligence
- Lost devices/Stolen devices, unless the theft claim is accompanied by a police report
- Lost or damaged power cord

**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. 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 prior to an incident. Coverage provides for one (1) incident per year. The second incident is covered with a $50 deductible. The cost of repair/replacement of damaged device beyond two (2) incidents 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 a lost or damaged charger at an approximate cost of $35.

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,payment options, or waivers. 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 1:1 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 252 ("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 WCASD network and Internet. This topic is covered throughout the K-12 library and technology curricula. Additionally, this topic is covered in 6th and 9th-grade orientation programs.

B. ACCEPTABLE/UNACCEPTABLE USE

1. Users are personally responsible for compliance with these requirements at all times when using the WCASD network and Internet.
2. The following are examples of unacceptable uses. However, WCASD 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 WCASD 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. WCASD 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. WCASD has access to all network activity to ensure compliance with WCASD 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, WCASD 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. Computer 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 Google or 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:

WCASD-1XWMM (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 5-10 minutes, 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 Google or 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 Google or 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 has also installed software that automatically creates a virtual private network (VPN) when used off-site for filtering and reporting by tunneling Internet traffic through the district's network. Parents/legal guardians may wish to use additional Internet filters at home. Many Internet Service Providers (ISP) have Parental Control settings; contact your ISP for information about how to use these settings. However, the additional controls must not interfere with the ability of our software to create the VPN tunnel back to the district's network.

Printing

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 Schoology, a Google 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. If the computer cannot directly connect to a printer, a second alternative is to use Google Cloud Print which works with a wide variety of printers. 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. For additional help information, students can refer to the "Adding a Wireless Printer" document in the student documentation folder on their desktop.

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 in grades 6-12, 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 or by calling the Office of Technology at 484-266-1050 or emailing one2one@wcasd.net.

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, however, rest assured that we have had a program in place for several years that has helped us develop these guidelines. Typically damage and theft are the biggest worries which are why we purchase the warranty and accidental damage coverage. Over the years and many thousands of computers distributed, we have had very few incidents of theft. That is not to say that damage and theft couldn't occur, but our experience has given us some degree of confidence that students are conscientious in taking care of their computer.

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 1:1 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 Business Office and Office of Technology as they are only trying to protect the district's investment in the 1:1 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. We urge parents to consider the Device Protection Plan as a means to reduce the chances of financial exposure.

QUESTIONS AND CONCERNS

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

Email: one2one@wcasd.net

Telephone: 484-266-1050

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.

POLICY 252 - STUDENT ACCEPTABLE USE OF INTERNET, COMPUTERS AND NETWORK RESOURCES

Purpose

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

The district has established learning standards to optimize the use of technology for teaching and learning:

- Digital Citizenship - Students use technology in responsible, respectful ways to contribute to discussions and provide solutions to issues affecting our society.
- Critical Thinking - Students use various types of reasoning aligned with technology to make judgments and informed decisions and to solve problems.
- Creativity - Students use a wide range of technologies in creative ways to express themselves, generate new ideas, solve problems and present solutions.
- Communication - Students use digital media and environments to articulate thoughts and ideas effectively to support individual and group learning.
- Information Literacy - Students apply digital tools to access, manage, evaluate, and use information.
- Collaboration - Students collaborate with peers and others employing a variety of environments and media.

The district provides students 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 including accounts and technology licensed by the district must be used for district business or academic purposes. All students must comply with this policy and all other applicable district policies, procedures and rules contained in this policy, as well as Internet Service Provider (ISP) terms, local, state and federal laws.

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, computer image 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.

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. Students 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, as well as accounts and technology licensed by the district. The district reserves the right to monitor, track, and log network access and use; monitor fileserver space utilization by students; 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 that the district-provided computers, Internet and other network resources must be used for district business or academic purposes, and that all students must comply with this policy and all other applicable district policies, procedures and rules contained in this policy, as well as Internet Service Provider (ISP) terms, local, state and federal laws. Students shall immediately report any violations or suspicious activities to the Superintendent or designee.

The Board establishes the following materials, in addition to those stated in law and defined in this policy, that are inappropriate for access by minors:[4]

1. Defamatory.
2. Lewd, vulgar, or profane.
3. Threatening.
4. Harassing or discriminatory.[9][10][11]
5. Bullying.[12]
6. Terroristic.[13]

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 district

may decrypt and inspect encrypted Internet traffic and communications to ensure compliance with this policy. The technology protection measure shall be enforced during use of computers with Internet access.[3][4][14]

Upon request by a student, 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 student may appeal the denial to the Superintendent or designee for expedited review.[3][14][15]

Delegation of Responsibility

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

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

Students using 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][16]

1. Utilizing a technology protection measure that blocks or filters Internet access for students and 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 students and other district users.

The Superintendent or designee shall develop and implement administrative guidelines that ensure students, staff, and parents/guardians 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][17]

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

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

Guidelines

Internet Access Opt-Out

Parents/Guardians of students in elementary school (K-5) may decide not to allow their child to access the Internet while at school by completing Parent Opt-Out Administrative Guideline 252-AG-1. If at any time during the school year parents/guardians would like to rescind their decision and change their permission, they must let the school know in writing.

Safety

It is the district's goal to protect users of the network from harassment and unwanted or unsolicited electronic communications. Any student who receives threatening or unwelcome electronic communications or inadvertently visits or accesses an inappropriate site shall report such immediately to a teacher or administrator. Students 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][16]

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

Students 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. Nonschool related work.

4. Product advertisement or political lobbying.
5. Bullying/Cyberbullying.[12][17]
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.[18]
9. Access by students to material that is harmful to minors or is determined inappropriate for students 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.[19]
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. Students shall not reveal their passwords to another individual.
2. Students are not to use a computer that has been logged in under another student's or employee's name.
3. Any student identified as a security risk or having a history of problems with other computer systems may be denied access to the network or may be subject to special usage arrangements for accessing technology resources.

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.[19][20]

Consequences for Inappropriate Use

Students shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.[14]

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.[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.[6][7][8]

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. Pol. 103
10. Pol. 103.1
11. Pol. 104
12. Pol. 249
13. Pol. 218.2
14. 24 P.S. 4604
15. 24 P.S. 4610
16. 47 CFR 54.520
17. 24 P.S. 1303.1-A
18. Pol. 237
19. Pol. 814
20. 17 U.S.C. 101 et seq

24 P.S. 4601 et seq
Pol. 220
Pol. 352
Pol. 814
Pol. 815.1
Pol. 815.2
Pol. 815.3
Pol. 815.4

POLICY 815.3 LENDING TECHNOLOGY EQUIPMENT

Purpose

Laptops, handhelds and other portable electronic equipment make it possible for staff to access electronic resources and perform mandatory administrative and instructional tasks from any location and for students to extend learning in the classroom, beyond the normal school day and outside of the school building. This policy establishes procedures for the provision of district-owned portable electronic equipment (equipment) for educational purposes.

Definition

Portable electronic equipment is any device that can be transported by the user and used in different environments. Such equipment is considered to be loaned if it is removed with authorization from the district premises for any length of time.

Authority

The Board establishes that equipment must be used for educational purposes only in accordance with all applicable Board policies. The use of equipment for personal purposes is prohibited. Furthermore, equipment shall not be loaned if the loan will cause a disruption in the regular educational program.

Guidelines

The user must sign 815.3-AG-1, Technology Equipment Checklist, prior to receiving equipment as verification of the identification of equipment and other accessories. The user is responsible for the return of all equipment and accessories as specified on the checklist in good working order.

Users shall follow the guidelines described in documentation provided by the Office of Technology. Such documentation will be provided to each user at the time the equipment is received and will be available on the district website.

If the equipment requires repair, the user shall not personally attempt repairs, but will report the problem and return the equipment to district technical support staff for diagnosis. The user shall be responsible for repair costs if the equipment is damaged due to misuse, accident, modification, unsuitable physical or operating environment or improper maintenance, provided the repairs are not covered by warranty. The user will not be responsible for the cost of normal repairs.

The district will not be obligated to provide more than one (1) computer to each employee except in a case of a medical requirement as documented by the user's physician.

The user is wholly liable for the full replacement cost of all lost and/or damaged equipment while in his/her possession; this also applies to the transporting of the loaned equipment between school and the home of the user.

If the loaned equipment was purchased by the district with extended warranty and accidental damage protection, the user must have already satisfied any cost-sharing conditions imposed by the district in order to benefit from the coverages afforded in the event of damage. No student shall be denied use of

district equipment because of financial reasons. Coverage does not include damage inflicted intentionally or through neglect, and these determinations are made at the sole discretion of the district.

For equipment not purchased with extended warranty and accidental damage insurance, the district's insurance policy is not in effect while the equipment is out of the district. Users should check their homeowner's policy to determine whether their insurance covers the equipment if damaged or stolen.

If equipment is lost or stolen, the loss or theft must be reported to the Technology Department within five (5) working days and, if the equipment was stolen, with a copy of the police report. If the equipment is not covered by district insurance, the user shall take action to reimburse the district for the lost or stolen equipment at the full replacement cost of the equipment within four (4) weeks of the report. Failure of a staff member to reimburse the district as specified shall result in the cost of the equipment being deducted from his/her paycheck.

The district shall not be responsible for any data/files left on a computer when it is returned. The district has the right to erase all files on a hard drive after return of the equipment, unless otherwise prohibited by law.

The user shall not make unauthorized copies of any copyrighted software that may be present on a computer nor load unauthorized copies of any other copyrighted software onto the computer.

Technical support shall not be provided by district technology staff outside of normal working hours or off the district premises.

The district may request immediate return of the equipment for any reason or at any time.

The user must return the equipment prior to leaving the district. Staff members must return equipment with the signed checklist prior to receipt of final paycheck. Students must return the equipment within seven (7) working days after requested by the district. The district shall take action to recover unreturned equipment which may include reporting the equipment as stolen to the police.

The user shall indemnify and hold harmless the district, its agents and employees from and against all claims, suits, actions, damages or causes from action arising from personal injury, loss of life or damages to property or both resulting directly or indirectly from the use of district equipment.

Delegation of Responsibility

School administration shall ensure that no equipment leaves the premises without proper documentation.

The Office of Technology shall maintain records of loaned equipment, equipment repairs and loss.

The Superintendent or his/her designee shall determine who may participate in the technology equipment loan program.

Legal

Pol. 000	Pol. 252	Pol. 710
Pol. 110	Pol. 352	Pol. 812
Pol. 224	Pol. 708	Pol. 815