

Pueblo County School District 70

Assigned Technology Device Handbook

Terms of Use

Terms

You will read and sign Pueblo County School District 70's (the District) Assigned Technology Device Use Agreement. You will comply at all times with the District's Assigned Technology Device Handbook and the Student Use of the Internet and Electronic Communications Acceptable Use Policy (AUP), incorporated herein by reference and made a part hereof for all purposes. Any failure to comply may terminate your rights of possession effectively immediately and the District may repossess the property.

Title

Legal title to the property is the District and shall at all times remain in the District. Your right of possession and use is limited to and conditioned upon your full and complete compliance with this Agreement and the Assigned Technology Device Parent-Student Handbook.

Loss or Damage

Insurance against loss or damage is available and highly recommended, but not mandatory. If you choose **not** to purchase insurance and the device is damaged, lost or stolen, you are responsible for all repair or replacement costs.

Loss or theft of the property must be reported to the District by the next school day after the occurrence. In case of theft, vandalism, and other criminal acts, a **police or sheriff report must be filed by the student or parent within 24 hours of the occurrence. Incidents that occur off campus must be reported to the local police or sheriff (depending on the location of incident) by the parent and a copy of the report must be brought to the school by the next school day.**

A table of estimated pricing for a variety of repairs and replacement cost is available upon request. Seniors must clear all records and pay all fees before participating in graduation ceremonies.

Repossession

If you do not timely and fully comply with all terms of this Agreement and the Assigned Technology Device Handbook, including the timely return of the property, the District shall be entitled to declare you in default and come to your place of residence, or other location of the property, to take possession of the property.

Term of Agreement

Your right to use and possession of the property terminates not later than the last day of the school year unless earlier terminated by the District or upon withdrawal from the District. A fee of \$ 10 per day may be assessed for devices not returned according to the terms herein.

Appropriation

Your failure to timely return the property and the continued use of it for non-school purposes without the District's consent may be considered unlawful appropriation of the District's property.

- If a transfer to another school takes place, you will have 48 hours to return the device to its home school.
- Seniors must clear ALL records and pay all technology related fees before participating in graduation.

Insurance

Insurance against loss or damage is available and highly recommended, but not mandatory. If you elect to enroll in Technology Device Insurance, a non-refundable insurance fee must be paid annually.

Damage, Loss or Theft

- In case of theft, vandalism, and other criminal acts, **a police or sheriff report must be filed by the student or parent within 24 hours of the occurrence. Incidents happening off campus must be reported to the local police or sheriff (depending on location of incident) by the parent and a copy of the report be brought to the school by the next business and/or school day.**
- Auto or home insurance may be billed for any difference or unrecoverable cost to the District.
- If you choose **not** to purchase insurance and the device is damaged, lost or stolen, the parent/guardian is financially responsible for all repair or replacement costs.

Deliberate Damage or Neglect

All repairs are based on the current cost the District must pay any approved manufacturer or provider to replace damaged devices and parts and are subject to change based on manufacturer's current price list.

The use of stickers, altering, or writing on carrying cases or devices is not allowed and will be charged for removal.

Borrowing and Loaning Devices

The District is committed to the importance of a student being able to continue with her/his work when a device is experiencing problems. To assist with this problem, the District will provide a temporary device for student use. The terms of the District's signed AUP, Device Handbook and Use Agreement apply to any temporarily assigned device. The student's advisory will be contacted to assist with any classroom or instructional concerns if the District is unable to provide a temporary device.

- Do NOT loan devices or other equipment to other students.
- Do NOT borrow a device from another student.
- Do NOT share passwords or usernames with others.

Internet Safety and Student Data Privacy

The District will use technological measures to ensure that District provided technology accounts, devices and educational resources are used appropriately and responsibly by students. The District will provide blocking and content filtering technology, as defined by the Board of Education's AUP (JS*), and in compliance with the Children's Internet Protection Act (CIPA), for all District devices having Internet or electronic communications access. Students are in violation of District policy if they access these sites through proxies. Parents may want to monitor or restrict home access to the Internet if blocking/filtering of content has been compromised.

The District, in compliance with the Federal Educational Rights and Protection Act (FERPA) and the Colorado Student Data and Transparency Act (HB16-1423), will develop policies and procedures that prevent unauthorized access and disclosure of or access to student information.

For more information about Internet safety, please go to www.isafe.org.

General Rules

Operating System

Configurations

Altering or modifying core system settings, original District pre-set software image and/or taking apart the device for access to internal components is prohibited and subject to a **\$50 Re-Imaging and/or Repair Fine** in addition to any cost of necessary repairs to affected components.

- Do not attempt to gain access to or modify any operating system files, administrative settings, application files and/or file permissions without direct authorization from an IT system administrator.
- Do not delete any folders or files that you did not create or that you do not recognize. Deletion of certain files may result in failures, interfere with your ability to complete work and affect your grades.

Screensavers and Unauthorized Software

- Inappropriate media may not be used as a screensaver and custom screensavers may only be applied to personal profile. Passwords on screensavers and power-on screen are not to be used.
- Presence of weapons, pornographic materials, inappropriate language, alcohol, drug and/or gang related symbols or pictures will result in disciplinary actions.
- Do not bypass or attempt to bypass any of the District's security or content filtering safeguards.
- Do not download or install any unauthorized software or install any unauthorized hardware.
- There will be a **\$50 Re-Imaging Fine** for the removal of any of the above.

Sound

- Sound will be muted at all times unless permission is obtained from the teacher for instructional purposes.
- No headphones except for instructional purposes or permitted by instructor/teacher.

Music

- Music and games may be downloaded using approved software outside of school hours.
- All software loaded on the system must be District approved.

Transporting Devices

- Devices must be transported in the District provided case.
- Devices must be shut down and stored in a safe location when not being utilized.

Acceptable Use of Technology Resources

Students must comply at all times with the District's Student Use of the Internet and Electronic Communications Acceptable Use Policy (JS*). These guidelines are provided here so that students and parents are aware of the responsibilities students accept when they use District owned device hardware, software, stored data and text, electronic mail (email), databases, device media, digitized information, communications technologies and Internet access. In general, this requires efficient, ethical and legal utilization of all technology resources.

1. Expectations

- a. Student use of devices, other technology hardware, software and networks including the Internet is only allowed when supervised or granted permission by a staff member.
- b. All users are expected to follow existing copyright laws. Copyright guidelines are posted and/or available in the media center of each campus as well as posted on the District website.

- c. Although the District has an AUP in place, students are expected to notify a staff member whenever they encounter information or messages that are inappropriate, dangerous, threatening, or make them feel uncomfortable.
- d. Students who identify or know about a security problem are expected to convey the details to their teacher or school administrator without discussing it with other students.

2. Unacceptable conduct includes, but is not limited to the following:

- a. Using the network for illegal activities, including copyright, license or contract violations, downloading inappropriate materials, viruses, and/or software, such as but not limited to hacking and host file sharing software.
- b. Using the network for financial or commercial gain, advertising, or political lobbying.
- c. Accessing or exploring on-line locations, materials, or social networking sites that do not support the curriculum and/or are inappropriate for school assignments or class time, such as but not limited to pornographic sites, Facebook, Skype, and Twitter. Violation may result in forfeit of the device for the remainder of the academic school year.
- d. Vandalizing and/or tampering with equipment, programs, files, software, system performance or other components of the network. Use or possession of hacking software is strictly prohibited.
- e. Causing congestion on the network or interfering with the work of others, e.g., chain letters or broadcast messages to lists or individuals.
- f. Intentionally wasting finite resources, i.e., on-line time, streaming music, gaming, unauthorized access anywhere on the network.
- g. Revealing the home address or phone number of one's self or another person.
- h. Invading the privacy of other individuals.
- i. Using another user's account, password, or ID card or allowing another user to access your account, password, or ID.
- j. Coaching, helping, observing or joining any unauthorized activity on the network.
- k. Forwarding/distributing E-mail messages without permission from the author.
- l. Posting anonymous messages or unlawful information on the system.
- m. Engaging in sexual harassment or using objectionable language in public or private messages, e.g., racist, terroristic, abusive, sexually explicit, threatening, stalking, demeaning or slanderous.
- n. Falsifying permission, authorization or identification documents.
- o. Obtaining copies of, or modifying files, data or passwords belonging to other users on the network.
- p. Knowingly placing a software virus on the District device or network.
- q. The use of recording devices such as the camera and microphone may not be used at school without permission from a teacher for a specified activity. Any use of the camera or microphone to record people without their knowledge or copy materials that are not allowed to be copied is forbidden.

Guidelines for Device Care

DO NOT

- leave your device in extreme weather conditions (in the car or on the field). Some components are susceptible to extreme temperatures and can be easily damaged.
- eat, drink, shower, use hair or nail products near devices at any time.
- operate devices on a non-hard surface such as your lap, bed, a blanket or pillow. The fan and heat sink must have proper air flow.
- “drop” the carrying case with device on the floor, even if it’s inches from the ground.
- apply personal markings and/or stickers to your device or carrying case.
- remove District or manufacturer’s stickers. This action is subject to fines.
- overstuff your device’s carrying case. This can result in the keyboard creating impressions on the LCD of the device and damage that is not covered under the current warranty.
- leave your device or case unattended.
- ignore lost or stolen device and/or hardware.
- be afraid to report damage to your device and/or device hardware.
- install banned or unapproved software, including additional anti-virus software.
- tightly wrap cords around your AC Adapter/Power Supply as wires may become frayed or weakened over time resulting in required replacement.
- use Goof Off, Windex or other harsh chemicals to clean your device.

DO

- store your device in a temperate, safe and secure location when not in use.
- use a clean, flat surface or approved lap tray/table with adequate ventilation to operate your device.
- store your device in the supplied case and carefully “set” the case with device down on any hard surface.
- decorate your case with ribbon, shoe laces, or other non-permanent selections.
- report peeling stickers to your local Electronic Repair Center (ER) for replacement.
- purchase a backpack for transporting books and other items that do not properly fit in your case.
- store your device in your locker or other temperate, secure location when not in use.
- report loss or theft immediately to your school’s security office.
- report damage to device and/or hardware to your local ER. Failure to report damage may void time sensitive coverage and assume negligence.
- install personal printers, ISP software, and other storage devices.
- loosely wrap the ends around the base of your adapter or “charger.”
- use microfiber or LCD cloths and canned air to clean your device.
- use Goo Gone to remove labels or stickers from your device.
- **Respect and take care of your device. It is yours while you remain at this school!**

Tips for Parents

Computing and technology devices are an educational resource or tool. The District strives to prepare all students for a future in the global workplace. Our children will be faced with Internet and technology distractions in everything they do in the world today. The District is preparing our students to stay focused optimally channel those distractions.

Parents are still in control and have the ability to:

1. Communicate with your children and set device limits that are age-appropriate for your child.

Here are some examples:

- a. I will not give out personal information such as my last name, address, telephone number, parent's work address/telephone number, or the name and location of my school without my parent's permission.
 - b. I will tell my parents right away if I come across any information that makes me feel uncomfortable.
 - c. I will never agree to get together with someone I "meet" online without first checking with my parents. If my parents agree to the meeting, I will be sure that it is in a public place and bring my mother or father along.
 - d. I will never send a person my picture or anything else without first checking with my parents.
 - e. I will not respond to any messages that are mean or in any way make me feel uncomfortable. It is not my fault if I get a message like that. If I do I will tell my parents right away so that they can contact the online service.
 - f. I will talk with my parents so that we can set up rules for going online. We will decide upon the time of day that I can be online, the length of time I can be online, and appropriate areas for me to visit. I will not access other areas or break these rules without their permission.
2. Limit the hours during the day that your child is on the device.
 3. Physically monitor student activity on the device.
 4. We encourage parents to have their student's login and password in order to monitor their child's device profile, as well as their selected Learning Management System (LMS) assignments. If students refuse to share, their LMS password can be reset at a parent's request.
 5. Modify security settings on the device- Contact the school's local Electronic Repair Center (ER) for more information.
 6. Call your Internet Service Provider (ISP) for assistance with blocking sites on your home network.