TECHNOLOGY

Applications, Protocols, Procedures

Date: July 1, 2018

APPENDIX B

TECHNOLOGY

TABLE OF CONTENTS

BYOD ACCESS AGREEMENT FORM

CPS Board Policy 3620F

INTERNET ACCESS CONDUCT AGREEMENT FORM

CPS Board Policy 3612F

The Colstrip Public Schools will strive to provide each enrolled student the opportunity to achieve the maximum of his or her potential within the limits of the elementary and secondary curriculum, so that each person may realize his/her personal worth and dignity to self and to society. The implementation of technology as a tools enhances student opportunities to maximize their potential.

Strategic Planning & Technology

Colstrip Public Schools' Board and Staff Leadership Team embrace the method of strategic planning as a continual and ongoing process to set the direction of the District for years to come. This is not a "strategic planning project" that is completed. Adoption of a strategic plan is an affirmation of the general intent and direction articulated by the Core Ideology, Envisioned Future and Goals and Strategic Objectives. It is understood that progress toward achieving strategic objectives will be assessed, and the plan will be updated based on achievement and changes in the needs of the children served by the Colstrip School District. The CPS Strategic Plan is available in its entirety on the District Website located at: http://colstrippublicschools.org/; however, Goal Area 5 specifically outlines future applications to technology.

CPS Goal Area 5: Technology

Statement of Intended Outcome, Five Years: Colstrip Public Schools has incorporated technology into all aspects of its educational offerings in such a manner as to prepare our students for a global environment. We have done this in a systematic manner to ensure that our staff are comfortably utilizing technology through professional development opportunities and that our students are benefiting from the use of technology and other advancements, while at the same time educating students and staff about the ethical and accountability issues associated with the use of technology.
One to Two Year Strategic Objectives:

1. We will enhance opportunities for staff to become proficient in technology equipment and applications that enhance student learning.
2. We will provide enhanced opportunities to make technology equipment and applications that directly relate to our students and/or enhanced learning opportunities available to students, parents and community members.
3. We will increase opportunities for students to utilize contemporary technology devices and application to enhance student learning.

Access to Electronic Information

CPS Board Policy 3612

The District makes Internet access and interconnected computer systems available to District students and faculty. The District provides electronic networks, including access to the Internet,

as part its instructional program and to promote educational excellence by facilitating resource sharing, innovation, and communication.

The District expects all students to take responsibility for appropriate and lawful use of this access, including good behavior on-line. The District may withdraw student access to its network and to the Internet when any misuse occurs. District teachers and other staff will make reasonable efforts to supervise use of network and Internet access; however, student cooperation is vital in exercising and promoting responsible use of this access.

Curriculum

Use of District electronic networks will be consistent with the curriculum adopted by the District, as well as with varied instructional needs, learning styles, abilities, and developmental levels of students, and will comply with selection criteria for instructional materials and library materials. Staff members may use the Internet throughout the curriculum, consistent with the District's educational goals.

Acceptable Uses

Educational Purposes Only. All use of the District's electronic network must be: (1) in support of education and/or research, and in furtherance of the District's stated educational goals; or (2) for a legitimate school business purpose. Use is a privilege, not a right. Students and staff members have no expectation of privacy in any materials that are stored, transmitted, or received via the District's electronic network or District computers. The District reserves the right to monitor, inspect, copy, review, and store, at any time and without prior notice, any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage.

Unacceptable Uses of Network

The following are considered unacceptable uses and constitute a violation of this policy:

- Uses that violate the law or encourage others to violate the law, including but not limited to transmitting offensive or harassing messages; offering for sale or use any substance the possession or use of which is prohibited by the District's student discipline policy; viewing, transmitting, or downloading pornographic materials or materials that encourage others to violate the law; intruding into the networks or computers of others; and downloading or transmitting confidential, trade secret information, or copyrighted materials.
- Uses that cause harm to others or damage to their property, including but not limited to engaging in defamation (harming another's reputation by lies); employing another's password or some other user identifier that misleads message recipients into believing that someone other than you is communicating, or otherwise using his/her access to the network or the Internet; uploading a worm, virus, other harmful form of programming or vandalism; participating in "hacking" activities or any form of unauthorized access to other computers, networks, or other information.

- Uses that jeopardize the security of student access and of the computer network or other networks on the Internet.
- Uses that are commercial transactions. Students and other users may not sell or buy anything over the Internet. Students and others should not give information to others, including credit card numbers and social security numbers.
- Each District computer with Internet access shall have a filtering device that blocks entry to visual depictions that are (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the Superintendent or designee. The school will also monitor the online activities of students, through direct observation and/or technological means, to ensure that students are not accessing such depictions or other material that is inappropriate for minors. The Superintendent or designee shall enforce the use of such filtering devices.
- The term "harmful to minors" is defined by the Communications Act of 1934 (47 USC Section 254 [h][7]), as meaning any picture, image, graphic image file, or other visual depiction that:
- taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
- 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 a lewd exhibition of the genitals;
- taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.
- Filtering should only be viewed as one of a number of techniques used to manage student's access to the Internet and encourage acceptable usage. It should not be viewed as a foolproof approach to preventing access to material considered inappropriate or harmful to minors.
- Filtering should be used in conjunction with:
    - Educating students to be "Net-smart";
    - Using recognized Internet gateways as a searching tool and/or homepage for students, in order to facilitate access to appropriate material;
    - Using "Acceptable Use Agreements";
    - Using behavior management practices for which Internet access privileges can be earned or lost; and
    - Appropriate supervision, in person and/or electronically.

- The system administrator and/or building principal shall monitor student Internet access.

Confidentiality of Student Information

Personally identifiable information concerning students may not be disclosed or used in any way on the Internet without the permission of a parent or guardian or, if the student is 18 or over, the permission of the student himself/herself. Users should never give out private or confidential information about themselves or others on the Internet, particularly credit card numbers and social security numbers. A supervising teacher or administrator may authorize the release of directory information, as defined by law, for internal administrative purposes or approved educational projects and activities.

Internet Access Conduct Agreements

Each student and his/her parent(s)/legal guardian(s) may be required to sign and return to the school at the beginning of each school year the Technology Resources User Agreement prior to having access to the District's computer system and/or Internet Service.

Warranties/Indemnification

The District makes no warranties of any kind, express or implied, in connection with its provision of access to and use of its networks and the Internet provided under this policy. The District is not responsible for any information that may be lost, damaged, or unavailable when using the network, or for any information that is retrieved or transmitted via the Internet. The District will not be responsible for any unauthorized charges or fees resulting from access to the Internet, and any user is fully responsible to the District and shall indemnify and hold the District, its trustees, administrators, teachers, and staff harmless from any and all loss, costs, claims, or damages resulting from such user's access to its computer network and the Internet, including, but not limited to, any fees or charges incurred through purchases of goods or services by the user. The user or, if the user is a minor, the user's parent(s)/legal guardian(s) agrees to cooperate with the District in the event of the school's initiating an investigation of a user's use of his/her access to its computer network and the Internet.

If any user violates this policy, the student's access may be denied, if not already provided, or withdrawn and he/she may be subject to additional disciplinary action. The system administrator and/or the building administrator will make all decisions regarding whether or not a user has violated this policy and any related rules or regulations and may deny, revoke, or suspend access at any time, with his/her/their decision being final.

Acceptable Use of Networks

CPS Board Policy 3612P

All use of electronic networks shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. These procedures do not attempt to state all required or proscribed behaviors by users. However, some specific examples are provided. The failure of any user to follow these procedures will result in the loss of privileges, disciplinary action, and/or appropriate legal action.

Terms and Conditions

Acceptable Use

Access to the electronic information, services and networks must be: (a) for the purpose of education or research and consistent with the educational objectives of the District; or (b) for legitimate business use.

Privileges

The use of the electronic information, services and networks is a privilege, not a right, and inappropriate use will result in cancellation of those privileges. The system administrator (and/or building principal) will make all decisions regarding whether or not a user has violated these procedures and may deny, revoke, or suspend access at any time. That decision is final.

Unacceptable Use

The user is responsible for his or her actions and activities involving the network. Some examples of unacceptable uses are:

- Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any federal or state law;
- Unauthorized downloading of software, regardless of whether it is copyrighted or de virused;
- Downloading copyrighted material for other than personal use;
- Using the network for private financial or commercial gain;
- Wastefully using resources, such as file space;
- Hacking or gaining unauthorized access to files, resources, or entities;
- Invading the privacy of individuals, which includes the unauthorized disclosure, dissemination, and use of information of a personal nature about anyone;
- Using another user's account or password;
- Posting material authored or created by another, without his/her consent;
- Posting anonymous messages;
- Using the network for commercial or private advertising;
- Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material; and
- Using the network while access privileges are suspended or revoked.

Network Etiquette

- The user is expected to abide by the generally accepted rules of network etiquette. These include but are not limited to the following:
- Be polite. Do not become abusive in messages to others.
- Use appropriate language. Do not swear or use vulgarities or any other inappropriate language.
- Do not reveal personal information, including the addresses or telephone numbers, of students or colleagues.

- Recognize that electronic mail (e-mail) is not private. People who operate the system have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.
- Do not use the network in any way that would disrupt its use by other users.
- Consider all communications and information accessible via the network to be private property.

No Warranties

The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages the user suffers. This includes loss of data resulting from delays, non-deliveries, missed deliveries, or service interruptions caused by its negligence or the user's errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

Indemnification

The user agrees to indemnify the District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District, relating to or arising out of any violation of these procedures.

Security

Network security is a high priority. If the user can identify a security problem on the Internet, the user must notify the system administrator or building principal. Do not demonstrate the problem to other users. Keep your account and password confidential. Do not use another individual's account without written permission from that individual. Attempts to log on to the Internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the network.

Vandalism

Vandalism will result in cancellation of privileges, and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any other network. This includes but is not limited to uploading or creation of computer viruses.

Telephone Charges

The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges, and/ or equipment or line costs.

Copyright Web Publishing Rules

Copyright law and District policy prohibit the republishing of text or graphics found on the Web or on District Websites or file servers, without explicit written permission.

- For each republication (on a Website or file server) of a graphic or text file that was produced externally, there must be a notice at the bottom of the page crediting the

original producer and noting how and when permission was granted. If possible, the notice should also include the Web address of the original source.

- Students and staff engaged in producing Web pages must provide library media specialists with e-mail or hard copy permissions before the Web pages are published. Printed evidence of the status of "public domain" documents must be provided.
- The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the Website displaying the material may not be considered a source of permission.
- The "fair use" rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.
- Student work may only be published if there is written permission from both the parent/guardian and the student.

Use of Electronic Mail

- The District's electronic mail system and its constituent software, hardware, and data files are owned and controlled by the District. The District provides e-mail to aid students and staff members in fulfilling their duties and responsibilities and as an education tool.
- The District reserves the right to access and disclose the contents of any account on its system without prior notice or permission from the account's user. Unauthorized access by any student or staff member to an electronic mail account is strictly prohibited.
- Each person should use the same degree of care in drafting an electronic mail message as would be put into a written memorandum or document. Nothing should be transmitted in an e-mail message that would be inappropriate in a letter or memorandum.
- Electronic messages transmitted via the District's Internet gateway carry with them an identification of the user's Internet "domain." This domain name is a registered domain name and identifies the author as being with the District. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of this District. Users will be held personally responsible for the content of any and all electronic mail messages transmitted to external recipients.
- Any message received from an unknown sender via the Internet should either be immediately deleted or forwarded to the system administrator. Downloading any file attached to any Internet-based message is prohibited, unless the user is certain of that message's authenticity and the nature of the file so transmitted.
- Use of the District's electronic mail system constitutes consent to these regulations.

Internet Safety

- Internet access is limited to only those "acceptable uses," as detailed in these procedures. Internet safety is almost assured if users will not engage in "unacceptable uses," as detailed in these procedures, and will otherwise follow these procedures.
- Staff members shall supervise students while students are using District Internet access, to ensure that the students abide by the Terms and Conditions for Internet access, as contained in these procedures.

- Each District computer with Internet access has a filtering device that blocks entry to visual depictions that are: (1) obscene; (2) pornographic; or (3) harmful or inappropriate for students, as defined by the Children's Internet Protection Act and determined by the Superintendent or designee.
- The district shall provide age-appropriate instruction to students regarding appropriate online behavior. Such instruction shall include, but not be limited to: positive interactions with others online, including on social networking sites and in chat rooms; proper online social etiquette; protection from online predators and personal safety; and how to recognize and respond to cyberbullying and other threats.
- The system administrator and building principals shall monitor student Internet access.

Bring Your Own Device (BYOD)

CPS Board Policy 3620

Purpose

Many students' lives today are filled with media that gives them mobile access to information and resources around the clock. Outside school, students are free to pursue their interest in their own way and at their own pace. The opportunities are limitless, borderless, and instantaneous. In an effort to put students at the center and empower them to take control of their own learning Colstrip Public Schools will allow students to use personal technology devices. Students wishing to participate must follow the responsibilities stated in the Acceptable Use Policy #3612 as well as the following guidelines.

Device Types

For the purpose of this program, the word "device" means all existing and emerging technology devices that can take photographs; record audio or video; input text; upload and download media; and transmit or receive messages or images. No gaming devices are allowed (to include but not limited to: Nintendo DS, PlayStation Portable PSP, etc.) Device type will be determined by the school administration.

Guidelines

1. Any student who wishes to use a personally owned electronic device within Colstrip Public Schools must read and sign both 3620F and 3612F forms. Parents are required to read and sign these same forms and submit to the appropriate school office.
2. The student takes full responsibility for his or her device and keeps it with him or herself at all times. The school is not responsible for the security of the student's device.
3. The student is responsible for the proper care of his or her personal device, including any costs of repair, replacement or any modifications needed to use the device at school.

4. The school administration reserves the right to inspect a student's personal device while it is in use at school during school hours.
5. Violations of any Board policies, administrative procedures or school rules involving a student's personally owned device may result in the loss of use of the device in school and/or disciplinary action.
6. The student must comply with a teacher's request to shutdown the device or close the device.
7. Personal devices shall be charged prior to bringing it to school and shall be capable of running off its own battery while at school.
8. The student may not use the devices to record, transmit or post photos or video of a person or persons on campus. Nor can any images or video recorded at school be transmitted or posted at any time without the express permission of a teacher.
9. During school hours, the student shall only use their device to access classroom related activities.
10. The student will use only the school's CPS Wi-Fi network access and no other wireless connections are allowed (for example 3G or 4G).

BYOD Frequently Asked Questions

CPS Board Policy 3620P

Parents

What if my child's device is stolen or damaged? What recourse can I take?
Students bring electronic communication devices to school at their own risk, just like any other personal items. The school will not be held responsible if an electronic device or other item is lost, stolen or misplaced. Some devices have a device locator; it is recommended that you enable this feature if possible.
Is it required that my child use the School wireless? Can they use their own 3G or 4G service?
Students with a personally owned device need to use the Colstrip Public School (CPS) wireless network.
My child is bringing a device to school for instructional purposes. Will they have access to things they will normally do with district equipment?
Your child will have access to any of the web-based software the school currently uses (databases, library search tools, etc.). Software may run differently on different devices for varying reasons.
As a parent am I required to add additional software (virus protection, filet, tracking device, etc.) to my child's device?
Virus protection of PC's is required. Device location software is not required but is always a good idea.
How will my sons/daughters device be used in the classroom?

Schools must challenge students with rigorous, personalized academic learning experiences that foster innovation and creativity. Students will engage in a cohesively integrated curriculum, access information, and apply it to solve authentic problems in a collaborative manner.

Students

I don't have my own electronic communication device to bring to school. Will I be penalized or miss out on instruction?
No, it is not mandatory for a student to bring a device, even if they do own one. Use of personal electronic devices will be optional. Keep in mind that learning can be enhanced greatly for the entire class even if only a handful of students have a device!
I have my device with me in class. How do I get on the Internet now?
Most devices will detect a wireless connection when you are near one. Most of the time devices will ask you if you would like to join the network when prompted. Choose CPS from the list.\
My device is not prompting me to choose a wireless network. Is there another way to connect?
In the settings menu on your device, there is usually an icon for a network. Go to this icon and choose guest from the list or prompt your computer to look for wireless network in range.
I cannot get my device to connect to the network. Can I get help from someone?
It is not the responsibility of your teacher or other staff to troubleshoot individual devices. Teachers utilizing a device for instructional purposes will make every attempt to assist students to connect and use their own devices. Students are expected to have a basic level of understanding and use of their own device before bringing it to school. Colstrip Public Schools cannot guarantee that all device types will be compatible with the tasks students are asked to perform or that they will be compatible with our network.
My device was stolen when I brought it to school. Who should I contact about this?
Colstrip Public Schools are not responsible for the theft of a device, nor are they responsible for any damage done to the device while at school. Any time a theft occurs, you should contact the school administrator to make him/her aware of the offense. Bringing your own device to school can be useful; however, some risks are involved as well. It is always a good idea to record the device's serial number to have in case of theft.
Why am I filtered on my own computer? Shouldn't I be able to see what I want on my own device?
Internet filtering is a requirement of all public schools. The Children Internet Protection Act (CIPA) requires all network access to be filtered regardless of the device you use to access it while in a public school. You own your own device, but the network you are using belongs to the school and Internet access will be filtered.
Am I still held accountable for the Acceptable Use Policy (AUP) I signed at the beginning of the school year even though this is my personal device?
Yes, students using a personally owned device must have both the Acceptable Use Policy (3612F) and the Bring Your Own Device (BYOD) policy (3620F) agreement signed by both the student and the parent/guardian.

Cell Phones and Other Electronic Equipment

CPS Board Policy 3630

Student possession and use of cellular phones, pagers, and other electronic signaling devices on school grounds, at school-sponsored activities, and while under the supervision and control of District employees is a privilege which will be permitted only under the circumstances described herein. At no time will any student operate a cell phone or other electronic device with video capabilities in a locker room, bathroom, or other location where such operation may violate the privacy right of another person.

Students may use cellular phones, pagers, and other electronic signaling devices on campus before school begins and after school ends, or as described in the student handbook. Students in grades 9-12 may also use such devices during the lunch period. These devices must be kept out of sight and turned off during the instructional day. Unauthorized use of such devices disrupts the instructional program and distracts from the learning environment. Therefore, unauthorized use is grounds for confiscation of the device by school officials, including classroom teachers. Confiscated devices will be returned to the parent or guardian. Repeated unauthorized use of such devices will result in disciplinary action.

Students who choose to register their privately owned device as required by Board Policy 3620, “Bring Your Own Device”, will be allowed to utilize their registered device as long as they follow guidelines as outlined in that policy as well as follow all requirements of Board Policy 3612, “Technology Acceptable use Policy”.

Fines Fees and Charges

CPS Board Policy 3520

Within the concept of free public education, the District will provide an educational program for students as free of costs as possible.

The Board may charge a student a reasonable fee for any course or activity not reasonably related to a recognized academic and educational goal of the District or for any course or activity taking place outside normal school functions. The Board may waive fees in cases of financial hardship.

The Board delegates authority to the Superintendent to establish appropriate fees and procedures governing collection of fees and asks the Superintendent to make annual reports to the Board regarding fee schedules. The Board also may require fees for actual cost of breakage and for excessive supplies used in commercial, industrial arts, music, domestic science, science, or agriculture courses.

The District holds a student responsible for the cost of replacing materials or property that are lost or damaged because of negligence. A building administrator will notify a student and parent regarding the nature of violation or damage, how restitution may be made, and how an appeal

may be instituted. The District may withhold a student's grades or diploma until restitution is made. The District may not refuse to transfer files to another district because a student owes fines or fees.

A school district may withhold the grades, diploma, or transcripts of a current or former pupil who is responsible for the cost of school materials or the loss or damage of school property until the pupil or the pupil's parent or guardian satisfies the obligation.

A school district that decides to withhold a pupil's grades, diploma, or transcripts from the pupil and the pupil's parent or guardian pursuant to the above paragraph shall:

- upon receiving notice that the pupil has transferred to another school district in the state, notify the pupil's parent or guardian in writing that the school district to which the pupil has transferred will be requested to withhold the pupil's grades, diploma, or transcripts until any obligation has been satisfied;
- forward appropriate grades or transcripts to the school to which the pupil has transferred;
- at the same time, notify the school district of any financial obligation of the pupil and request the withholding of the pupil's grades, diploma, or transcripts until any obligations are met;
- when the pupil or the pupil's parent or guardian satisfies the obligation, inform the school district to which the pupil has transferred;

A student or parent may appeal the imposition of a charge for damages to the Superintendent and to the Board.

For loss or damages, the student will be assessed not more than:

a. First (1st) year – full price if new when issued
b. Second (2nd) year – eighty percent (80%) of full price
c. Third (3rd) year – sixty percent (60%) of full price
d. Fourth (4th) year – forty percent (40%) of full price
e. Fifth (5th) year – twenty percent (20%) of full price
f. All subsequent years – ten percent (10%) of full price

Chromebooks

One To One

Colstrip Public Schools utilize a one-to-one chromebook concept to deliver the tools needed to maximize student learning. The term one-to-one is applies to programs that provide all students in a school, district, or state with their own laptop, netbook, tablet computer, chromebook or other mobile-computing device. At Colstrip Public Schools, one-to-one refers to one chromebook for every student.

Given that computers, technology, and the internet are rapidly redefining nearly every area of modern life—from education to communications to careers—one-to-one programs are motivated by the following rationales:

- Today's students need consistent, at-the-ready access to computing devices throughout the day and, ideally, at home.
- Teachers can only take full advantage of new learning technologies and online educational resources when all students are equipped with a computing device.
- Teaching technological literacy and computing skills needs to be a priority in today's schools.
- Equipping all students with computing devices and incorporating technology into every course is the surest way to take full advantage of new learning technologies and produce students who are technologically skilled and literate.

One-to-one computing environments are seen by many educators and reformers as the next logical step for schools. In schools without a one-to-one computing program, teachers may need to schedule computing time in advance, and—depending on a school's computing options and computer supply—scheduling conflicts can arise. Teachers may also need to postpone or modify certain lessons, and valuable instructional time can be eroded because students may need to be moved to a computer lab, it may take extra time to get shared computers configured properly, or the computers may not have the required software, for example.

In addition to avoiding many logistical issues associated with more limited or restrictive computing options, one-to-one programs give teachers greater flexibility in how they can use computers as instructional resources. For example, one-to-one programs:

- Allow all students to work online simultaneously in a class or to work collaboratively on a project that is hosted in the cloud.
- Allow teachers to use interactive, technology-assisted teaching strategies that require students to have a computing device. For example, teachers can pose questions to a class, and all students can respond using an online survey system. Instead of asking a question and picking one student to give an answer, teachers can get answers from all students in real time to see who has understood the material, who hasn't, and who made need extra help.
- Make it easier for students to save work on their own account.
- Allow teachers to use "course-management software" to organize a class or assign long-term projects or homework that require students to use a computer.
- Make it easier to find cheaper or more up-to-date learning materials for students (for example, textbooks can be expensive and can quickly become outdated) and to diversify the types of learning tools, materials, and readings teachers make available to students, such as interactive e-textbooks, digital simulations, self-paced online tests, video-editing applications, or multimedia software, for example.
- Make it easier—or possible—to use new or more innovative teaching strategies such as blended learning and "flipped classrooms" or to incorporate online courses into the learning options schools make available to students.

(Source: http://edglossary.org/one-to-one/)

At Colstrip Public Schools the distribution and use of chromebooks is different at each building and developmental level from dependent monitoring to independent use.

Pine Butte Elementary

At the elementary level, students are provided chromebooks for specific tasks and learning. Chromebooks are not sent home.The chromebooks are managed by the classroom teacher; therefore, there is no need for students to check out a chromebook. Students will be assigned the same chromebook by their classroom teacher just as they are a desk or textbook. Parents and students at the elementary level are still required to complete CPS Policy *3612F Internet Access Conduct Agreement* prior to on-line access and use. Many of the processes, procedures, administrative policies and guidelines listed in the Chromebook section of this Appendix will not apply to K-5 students; however, whenever levels of independent use are implemented, it is the expectation of the district that these processes, procedures, administrative policies and guidelines be followed by all students of Colstrip Public Schools.

Frank Brattin Middle School

During the transition years from middle school to high school, the one-to-one step in issuing chromebooks will take on many forms. It is the intent of Colstrip Public Schools to develop students, their understanding and responsibility for the independent use and access of a chromebook. To this end, chromebooks will be checked out to all students at school, but may not be permitted to travel home; the administration and staff will make this decision at the appropriate developmental level and time. Students and parents must complete the identified forms outlined in this appendix in order to gain access and permission for chromebook check out. Whenever levels of independent use are implemented, it is the expectation of the district that these processes, procedures, administrative policies and guidelines be followed by all students of Colstrip Public Schools.

Colstrip High School

All processes, procedures, administrative policies and guidelines are detailed for maximized independence and use of a chromebook for the applications of teaching and learning at Colstrip High School; therefore, all apply without restriction to 9-12 grade students.

Receiving Your Chromebook

Distribution of Chromebooks

All 6-12 grade students will be assigned a Chromebook that will be personally assigned to them for the entire time you attend Colstrip Public Schools, so it is very important for you to take care of it. The Chromebook will have your name and Graduation year on the Chromebook for easy identification.

All K-5 students will have access to a chromebook checked out to the classroom teacher. All students will have one-to-one access.

Important: Students and a parent/guardian must sign the Internet Access Conduct Agreement prior to picking up or using a Chromebook. Forms are available at your school's office as well as a codicil to this appendix (see Forms at the end of this document).

In addition, before authorization for network access can be granted, all users must successfully complete the Colstrip Public Schools #19 Internet Safety and Digital Citizenship curriculum basics. The curriculum basics will be provided during the first several days of school. Alternative trainings will be arranged by the building administration and provided by the district technology staff.

a. Cyberbullying
b. Privacy and Information Sharing
c. Social Networking Safety
d. Online Predator Safety

Transfer/New Student Distribution

All 6-12 grade transfers, new students or students that miss the early distribution can pick up their Chromebook in the Main Office at the Middle School or the Technology Support Center at the High School.

Important: Students and a parent/guardian must sign the Internet Access Conduct Agreement prior to picking up or using a Chromebook. Forms are available at your school's office as well as a codicil to this appendix (see Forms at the end of this document).

In addition, before authorization for network access can be granted, all users must successfully complete the Colstrip Public Schools #19 Internet Safety and Digital Citizenship curriculum basics. Alternative trainings will be arranged by the building administration and provided by the district technology staff.

e. Cyberbullying
f. Privacy and Information Sharing
g. Social Networking Safety
h. Online Predator Safety

Returning Your Chromebook

End of Year

Prior to the end of the year you will return your Chromebook to the Main office at the Middle School or the Technology Support Center at the High School. Seniors are required to return their Chromebook as part of senior checkout. Failure to turn in a Chromebook will result in the

parent/guardian being charged for the chromebook. See Fines, Fees and Charges section in this appendix or Board Policy 3520. There will also be a charge for any missing peripheral equipment such as the case, mouse, or power supply.

Transferring/Withdrawing Graduating Students

Students transferring out of or withdrawing from Colstrip Public Schools must turn in their Chromebooks, cases, power supplies, and any other equipment issued with the Chromebook to the Main Office at the Middle School or the Technology Support Center at the High School on their last day of attendance. Failure to turn in the Chromebook will result in the student being charged being charged for the chromebook. See Fines, Fees and Charges section in this appendix or Board Policy 3520. There will also be a charge for any missing peripheral equipment such as the case, mouse, or power supply.

Taking Care of Your Chromebook

Students are responsible for the general care of the Chromebook they have been issued by the school. Chromebooks that are broken or fail to work properly must be taken to the Main Office at the Middle School or the Technology Support Center at the High School as soon as possible so that they can be taken care of properly. District-owned Chromebooks should never be taken to an outside computer service for any type of repairs or maintenance.

General Precautions

Please help maintain the pristine condition of the Chromebooks. To that end please observe the following:

- Students should never leave their Chromebooks unattended except locked in their locker.
- No food or drink should be next to Chromebooks.
- Cords, cables, and removable storage devices must be inserted carefully into Chromebooks.
- Chromebooks should not be used or stored near pets.
- Chromebooks should not be exposed to extreme temperatures, such as leaving it in a car overnight.
- Chromebooks should not be used with the power cord plugged in when the cord may be a tripping hazard.
- Heavy objects should never be placed on top of Chromebooks.
- Chromebooks must remain free of any writing, drawing, or stickers. Do not attempt to reapply identifying tags originally applied to the Chromebook such as student name or CPS numbers. The Tech department will repair damaged or missing tags.

Cases

- Each student will be issued a protective case for his/her Chromebook that should be used whenever the Chromebook is being transported or not in use.

- Although the cases are reinforced to help protect the Chromebooks, they are not guaranteed to prevent damage. It remains the student's responsibility to care for and protect his/her device.

Carrying Chromebooks

- Always transport Chromebooks with care and in Colstrip-issued protective cases.
- Never lift Chromebooks by the screen.
- Never carry Chromebooks with the screen open.

Screen Care

The Chromebook screen can be damaged if subjected to heavy objects, rough treatment, some cleaning solvents, and other liquids. The screens are particularly sensitive to damage from excessive pressure.

- Do not put pressure on the top of a Chromebook when it is closed.
- Do not store a Chromebook with the screen open.
- Do not place anything in the protective case that will press against the cover.Make sure there is nothing on the keyboard before closing the lid (e.g. pens, pencils, etc).
- Only clean the screen with a soft, dry microfiber cloth or anti-static cloth.

CPS Tags

- All Chromebooks will be labeled with a Colstrip CPS tag. The CPS tag indicates the Chromebook is property of the Colstrip Public Schools and provides information that allows us to determine the name of the student to which the specific Chromebook has been assigned.
- CPS tags may not be modified or tampered with in any way.

Using Your Chromebook At School

Students are expected to bring a fully charged Chromebook to school every day and bring their Chromebooks to all classes unless specifically advised not to do so by their teacher.

If a student does not bring his/her Chromebook to school:

- A student may stop in the Main Office at the Middle School or the Technology Support Center at the High School and check out a loaned chromebook for the day.
- A student borrowing a Chromebook must sign a loan agreement and will be responsible for any damage to or loss of the issued device.
- The Technology Support Center will document the number of times a loaned chromebook is issued to each student for not having his/her own chromebook at school and will send reports to the building administration for those students that have more than one occurrence during the school year.

- Multiple occurrences of coming to school without one's chromebook may result in disciplinary action.
- The students that obtain a loaned chromebook will be responsible for returning the borrowed device before 3:45 p.m (2:45 p.m. on early out Thursday).
- If a loaned chromebook is not turned in on time, the Technology Support Center will submit a report to the building administrator.

Chromebooks being repaired

- Loaned chromebooks may be issued to students when they submit their school-issued chromebook for repair.
- A student borrowing a chromebook must sign a loan agreement and will be responsible for any damage to or loss of the loaned device.
- Chromebooks on loan to students having their devices repaired may be taken home.
- A member of the Student Technology Assistance Team/administration/technology staff will contact students when their devices are repaired and available for pick up.

Charging Chromebooks

- Chromebooks must be brought to school each day with a full charge.
- Students should charge their Chromebooks at home every evening.
- There will be a limited number of charging stations located in the school, available to students on a first-come-first-served basis.
- Optionally, students may take their dead Chromebooks to the Main Office at the Middle School or the Technology Support Center at the High School for charging. A completely dead Chromebook takes about 2 hours to fully charge so plan accordingly.
- It is recommended that students need not carry the AC Adapter power cord (charger) to school. If fully charged at home, the battery should last the entire day.

Backgrounds and Themes

- Inappropriate media may not be used as Chromebook backgrounds or themes. The presence of such media will result in disciplinary action.

Sound

- Sound must be muted at all times unless permission is obtained from a teacher.
- Headphones may be used at the discretion of the teachers.

Printing

- Students will be encouraged to digitally publish and share their work with their teachers and peers whenever possible.
- Students will be able to print from their Chromebooks to designated printers.

- Students may set up their home printers with the Google Cloud Print solution to print from their Chromebooks at home. Information about Google Cloud Print can be found at http://www.google.com/cloudprint.

Logging into a Chromebook

- Students will log into their Chromebooks using their school-issued Google Apps for Education account.
- Students should never share their account passwords with others, including faculty and staff.

Managing and Saving Your Digital Work With a Chromebook

- The majority of student work will be stored in Internet/cloud based applications and can be accessed from any computer with an Internet connection and most mobile Internet devices.
- Students should always remember to save frequently when working on digital media.
- The district will not be responsible for the loss of any student work.
- Students are encouraged to maintain backups of their important work on a portable storage device or by having multiple copies stored in different Internet storage solutions.

Using Your Chromebook Outside of School

Students are encouraged to use their Chromebooks at home and other locations outside of school. A WiFi Internet connection will be required for the majority of Chromebook use, however, some applications can be used while not connected to the Internet. Students are bound by the Colstrip Public Schools Policy *3612 District-Provided Access to Electronic Information, Services, and Networks, 3612P Acceptable Use of Electronic Networks* and *3612F Internet Access Conduct Agreement Form* wherever they use their Chromebooks.

Students are responsible for all aspects of network connection and printing outside of school.

Operating System and Security

Students may not use or install any operating system on their Chromebook other than the current version of ChromeOS that is supported and managed by the district.

Updates

- The Chromebook operating system, ChromeOS, updates itself automatically. Students do not need to manually update their Chromebooks.

Virus Protection

- There is no need for additional virus protection.

Content Filter

The district utilizes an Internet content filter that is in compliance with the federally mandated Children's Internet Protection Act (CIPA). All Chromebooks, regardless of physical location (in or out of school), will have all Internet activity protected and monitored by the district. If an educationally valuable site is blocked, students should contact their teachers to request that the site be unblocked.

Software

Google Apps for Education

- Chromebooks seamlessly integrate with the Google Apps for Education suite of productivity and collaboration tools. This suite includes Google Docs (word processing), Spreadsheets, Presentations, Drawings, and Forms.
- All work is stored in the cloud.

Chrome Web Apps and Extensions

- Students are allowed to install appropriate Chrome web apps and extensions from the Chrome Web Store.
- Students are responsible for the web apps and extensions they install on their Chromebooks. Inappropriate material will result in disciplinary action.
- Some web apps will be available to use when the Chromebook is not connected to the Internet.

Chromebook Identification

Records

- The district will maintain a log of all Chromebooks that includes the Chromebook serial number, CPS code, and name and ID number of the student assigned to the device.

Users

- Each student will be assigned the same Chromebook for the duration of his/her time at Colstrip Public Schools. Take good care of it!

Repairing/Replacing Your Chromebook

Chromebook Repair Locations

- All Chromebooks in need of repair must be brought to the Main Office at the Middle School or the Technology Support Center at the High School as soon as possible either for repair or replacement.

- If technical difficulties occur, technical support staff will use the “15-minute” rule. If the problem cannot be fixed in 15 minutes, the Chromebook will be restored to factory defaults. In a One-to-One environment it is very difficult for support staff to maintain a working environment for all if too much time is spent fixing every glitch that may arise. Restoring the Chrome OS will restore the device to the state in which the user originally received it. All student created files stored on an external miniSD card, USB flash drive, or Google Drive will be intact after the operating system is restored. All files saved on the chromebook that have been synced to Google Drive will be intact. However, all other data (music, photos, documents) stored on internal memory that has NOT been synced will not be restored unless the student requests that an attempt be made to salvage it.

Privacy Expectations

School-issued Chromebooks have been configured to optimize the educational experience for students and staff as well as protect students from harmful content per federally mandated guidelines.

On Campus Chromebook Use

- As mentioned, all devices on the school network go through a content filter that prevents students from accessing harmful content. This filter also logs user activity, including those websites accessed by the end user. The filtering policies are a requirement of the Children’s Internet Protection Act (CIPA).

Off Campus Chromebook Use

- Chromebooks will be filtered for the purpose of preventing students from accessing harmful content in a similar way they are filtered on school grounds.

At no time will any member of the Colstrip Public School staff have the ability to manipulate the Chromebook webcam in any way.

Appropriate Uses and Digital Citizenship

School-issued Chromebooks should be used for educational purposes and students are to adhere to the CPS Digital Citizenship Responsibility Policies and all of its corresponding administrative procedures at all times.

BYOD ACCESS AGREEMENT FORM

CPS Board Policy 3620F

Bring Your Own Device (BYOD)
Parent/Student User Agreement
(One signed agreement per student)

Return to School Office

As a student, I understand and will abide by School Board Policies #3612 and #3620. I further understand that any violation of these policies may result in the loss of my network and/or device privileges as well as other disciplinary action.

As a parent, I understand that my child will be responsible for abiding by School Board Policies #3612 and #3620. I have read and discussed these policies with my child and he/she understands the responsibility required in the use of their personal device under these policies.

Student Name: _____ Student Signature:_____ Date: _____

Parent Name: _____ Parent Signature: _____ Date: _____

Device Type/Description: _____

MAC (Hardware) Address: _____

Technology Service Verification Signature: _____ Date: _____

INTERNET ACCESS CONDUCT AGREEMENT FORM

CPS Board Policy 3612F

Parent/Student User Agreement
(One signed agreement per student)

Return to School Office

Technology offers vast, diverse, and unique resources to both students and staff members of Colstrip Public School District #19. The district's goal in providing this service to staff and students is to promote education excellence in schools by facilitating resource sharing, innovation and communication. Technology from this point forward is meant to include the computer, phone services or any other means of network communications. User refers to any student, district employee, or community member using the network services provided by Colstrip Public School District #19.

Access to computers and people all over the world includes the availability of material that may not be considered to be of educational value in the context of the school setting. Colstrip Public School District #19 believes that the benefits of using information and interaction made available on this worldwide network far outweigh the chance that a user will procure materials not consistent with the educational goals of the district. It is the district's intent to provide guided access and supervision for students using technology.

Technology access is coordinated through a complex association of government agencies and regional and state networks. In addition, the smooth operation of the network relies upon the proper conduct of the end users who must adhere to strict policies. These procedures are provided here so the user is aware of his/her responsibilities. Users are expected to utilize technology resources in an efficient, ethical and legal manner. If a user violates any of these expectations, his/her access may be terminated, future access may be denied, and disciplinary action may be warranted.

Terms and Conditions

Acceptable Use – Access to the electronic information, services and networks must be: (a) for the purpose of education or research and consistent with the educational objectives of the District; or (b) for legitimate business use.
Privileges – The use of the electronic information, services and networks is a privilege, not a right, and inappropriate use will result in cancellation of those privileges. The system administrator (and/or building principal) will make all decisions regarding whether or not a user has violated these procedures and may deny, revoke, or suspend access at any time. That decision is final.

Unacceptable Use – The user is responsible for his or her actions and activities involving the network. Some examples of unacceptable uses are:

a. Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any federal or state law;
b. Unauthorized downloading of software, regardless of whether it is copyrighted or
without virus;
c. Downloading copyrighted material for other than personal use;
d. Using the network for private financial or commercial gain;
e. Wastefully using resources, such as file space;
f. Hacking or gaining unauthorized access to files, resources, or entities;
g. Invading the privacy of individuals, which includes the unauthorized disclosure, dissemination, and use of information of a personal nature about anyone;
h. Using another user's account or password;
i. Posting material authored or created by another, without his/her consent;
j. Posting anonymous messages;
k. Using the network for commercial or private advertising;
l. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material; and
m. Using the network while access privileges are suspended or revoked.

Network Etiquette – The user is expected to abide by the generally accepted rules of network etiquette. These include but are not limited to the following:

a. Be polite. Do not become abusive in messages to others.
b. Use appropriate language. Do not swear or use vulgarities or any other inappropriate language.
c. Do not reveal personal information, including the addresses or telephone numbers,
d. of students or colleagues.
e. Recognize that electronic mail (e-mail) is not private. People who operate the system have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.
f. Do not use the network in any way that would disrupt its use by other users.
g. Consider all communications and information accessible via the network to be private property.

No Warranties – The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages the user suffers. This includes loss of data resulting from delays, non-deliveries, missed deliveries, or service interruptions caused by its negligence or the user's errors or omissions. Use of any information obtained via the Internet is at the user's own risk.

The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

Indemnification – The user agrees to indemnify the District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District, relating to or arising out of any violation of these procedures.

Security – Network security is a high priority. If the user can identify a security problem on the Internet, the user must notify the system administrator or building principal. Do not demonstrate the problem to other users. Keep your account and password confidential. Do not use another individual's account without written permission from that individual. Attempts to log on to the Internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the network.

Vandalism – Vandalism will result in cancellation of privileges, and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any other network. This includes but is not limited to uploading or creation of computer viruses.

Telephone Charges – The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges, and/ or equipment or line costs.

Copyright Web Publishing Rules – Copyright law and District policy prohibit the republishing of text or graphics found on the Web or on District Websites or file servers, without explicit written permission.

a. For each republication (on a Website or file server) of a graphic or text file that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission was granted. If possible, the notice should also include the Web address of the original source.

b. Students and staff engaged in producing Web pages must provide library media specialists with e-mail or hard copy permissions before the Web pages are published. Printed evidence of the status of "public domain" documents must be provided.

c. The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the Website displaying the material may not be considered a source of permission.

d. The “fair use” rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.

e. Student work may only be published if there is written permission from both the parent/guardian and the student.

Use of Electronic Mail

a. The District’s electronic mail system and its constituent software, hardware, and data files are owned and controlled by the District. The District provides e-mail to aid students and staff members in fulfilling their duties and responsibilities and as an education tool.

b. The District reserves the right to access and disclose the contents of any account on its system without prior notice or permission from the account’s user. Unauthorized access by any student or staff member to an electronic mail account is strictly prohibited.

c. Each person should use the same degree of care in drafting an electronic mail message as would be put into a written memorandum or document. Nothing should be transmitted in an e-mail message that would be inappropriate in a letter or memorandum.

d. Electronic messages transmitted via the District’s Internet gateway carry with them an identification of the user’s Internet “domain.” This domain name is a registered domain name and identifies the author as being with the District. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of this District. Users will be held personally responsible for the content of any and all electronic mail messages transmitted to external recipients.

e. Any message received from an unknown sender via the Internet should either be immediately deleted or forwarded to the system administrator. Downloading any file attached to any Internet-based message is prohibited, unless the user is certain of that message’s authenticity and the nature of the file so transmitted.

f. Use of the District’s electronic mail system constitutes consent to these regulations.

Internet Safety

2. Internet access is limited to only those “acceptable uses,” as detailed in these procedures. Internet safety is almost assured if users will not engage in “unacceptable uses,” as detailed in these procedures, and will otherwise follow these procedures.

3. Staff members shall supervise students while students are using District Internet access, to ensure that the students abide by the Terms and Conditions for Internet access, as contained in these procedures.

4. Each District computer with Internet access has a filtering device that blocks entry to visual depictions that are: (1) obscene; (2) pornographic; or (3) harmful or inappropriate for students, as defined by the Children’s Internet Protection Act and determined by the Superintendent or designee.

5. The district shall provide age-appropriate instruction to students regarding appropriate online behavior. Such instruction shall include, but not be limited to: positive interactions with others online, including on social networking sites and in chat rooms; proper online social etiquette; protection from online predators and personal safety; and how to recognize and respond to cyberbullying and other threats.

6. The system administrator and building principals shall monitor student Internet access.

On-line Education Component:

Before authorization for network access can be granted, all users must successfully complete the Colstrip Public Schools #19 Internet Safety and Digital Citizenship curriculum basics.

a. Cyberbullying
b. Privacy and Information Sharing
c. Social Networking Safety
d. Online Predator Safety

This agreement is for the sole purpose of clarification in accordance with Board Policy 3612 District Provided Access to Electronic Information, Services and Networks, 3620 Bring Your Own Device (BYOD). Violation of any policy or procedure is subject to disciplinary actions specified in the handbook. The system administrator reserves the right to terminate/restrict a user’s privileges as needed.

The District will only create network account(s) for minors if the Guardian signs the Consent Form. All network users are accepting the terms of all policies and procedures of Colstrip Pubic Schools #19 by logging into the District’s electronic network.

This Authorization for Electronic Network Access administrative procedure may be revised at any time by the District without prior notice. Please refer to the most current version of this procedure as posted on the District’s website.

Electronic Use Agreement

Student:

I have read the Authorization for Electronic Network Access and viewed the Internet Safety Basics component of the Internet Safety and Digital Citizenship curriculum. I understand that Internet sites are filtered and that use on a district computer or device and the district network may be monitored. I hereby agree to comply with the described conditions of acceptable use.

Student Name: _____ Student Signature:_____ Date: _____

Parent Name: _____ Parent Signature: _____ Date: _____

As the parent or guardian of the above named student, I have read the Authorization for Electronic Network Access and understand that Internet sites are filtered and that electronic information resource accounts may be monitored. I understand my child may be disciplined for inappropriate or unacceptable use of electronic information resources. I further understand that student use of the electronic information resource system is designed for educational purposes. I understand that it is impossible for the district to filter or restrict access to all inappropriate materials. I will not hold the District responsible for inappropriate or unacceptable materials my child may acquire on the network system.

I hereby give my permission and approve the issuance of an electronic account for my child.

Student Name: _____ Student Signature:_____ Date: _____

Parent Name: _____ Parent Signature: _____ Date: _____