Benton County School District (BCSD)
Technology Acceptable Use Policy (TAUP)

(2021-2022 School Year)

TERMS AND CONDITIONS FOR USE OF THE BCSD NETWORK AND TECHNOLOGY

All users of the BCSD's network and Internet access are required to adhere to the district's Technology Acceptable Use Policy (TAUP). The policy describes in detail the purpose of the district's network and the rules governing its use.

All users and the parents of all student users are required by the BCSD TAUP to sign a contract stating that they will abide by the policy while using the district's technology resources. The TAUP agreement form is located on the last page of this handbook and on the district web site. A new TAUP agreement must be filled out and signed in the presence of BCSD administration by a parent/guardian (responsible party) for each student and each device.

All users, including faculty and staff, must be aware that misuse of technology could result in disciplinary action by the BCSD officials including termination of employment or legal action by local, state and/or federal law enforcement officials.

It is, therefore, incumbent upon all who sign the Internet Use Contract to carefully read the BCSD TAUP and understand what is expected and the penalty for non-compliance.

The Benton County School District (BCSD) offers currently enrolled students, faculty and staff access to the school computer network through computer labs, district issued devices (chrome books, computers, etc.), networked and stand-alone computers. District technology equipment is provided for use in fulfilling curriculum objectives and quality enrichment activities. Personal electronic devices are only allowed to be connected to the district network with permission of district administration. This includes, but is not limited to personal computers, laptops, tablets, chrome books, and smart phones.

Children's Internet Protection Act (CIPA)

The BCSD follows the Children's Internet Protection Act (CIPA) and will comply with any additional state and federal regulations that pertain to technology use within the district and through use of the BCSD network infrastructure and servers that is forthcoming from the local, state and federal regulatory agencies.

The Children's Internet Protection Act (CIPA) is a federal law enacted by Congress to address concerns about access in schools and libraries to the Internet and other information. Among many other things, it calls for schools and libraries to have in place appropriate electronic filters to prevent children and adults from accessing and viewing inappropriate Internet content. For any school or library that receives discounts for Internet access or for internal connections, CIPA imposes certain requirements. The BCSD receives these discounts for Internet Access through the E-Rate program and therefore must follow CIPA.

NETWORK SECURITY – CIPA COMPLIANCE

Users have the responsibility to use computer and network resources for academic purposes only. Therefore, as mandated by CIPA, filtering and monitoring will be utilized on all computers accessing the Internet. Free email sites are blocked for all users. Faculty and staff must use District provided email and students will have access to Google email. The district is required by the State to archive (keep on file) all email going in and out. This is due to past litigations involving email and requirements for the district to produce email copies when requested by the courts.

Activities using the computer network in violation of Local, State, Federal or BCSD policies are strictly forbidden.

Students will not respond to unsolicited online contacts or reveal personal identifiable information over the network unless it meets District-approval (examples: ACT Registration, Scholarships or College Applications). This includes information about themselves as well as information about anyone else.

BCSD staff is prohibited from disclosing personal information about students on websites. Although teachers and other district personnel may reveal personal information about themselves over the network, they are strictly forbidden to disseminate any student information electronically to any source that has not met district approval. Information that is considered personal includes but is not limited to the following: student's full name, home address, Social Security number, personal telephone numbers, and any information relating to their health.

Because there are additional prohibitions with which users must comply, non-compliance with these regulations will result in disciplinary and/or legal actions taken by the BCSD authorities if deemed necessary.

COMPUTER NETWORK AND INTERNET USE RULES

Students and school personnel are responsible for good behavior on the school computer networks just as they are in a class- room or in a school hallway. Communications on the network are often public in nature. General school rules for behavior and communications apply. Within reason, freedom of speech and access to information will be honored.

In compliance with CIPA, all students (K-12) will be educated about appropriate online behavior, including interacting with other individuals on social networking websites, in chat rooms and in cyberbullying awareness and response. When using the Internet, all students will be closely monitored to prevent students from accidentally or otherwise accessing inappropriate material.

Computer access is a privilege, not a right, and is provided for students and staff to conduct research, fulfill course requirements and communicate with others when appropriate or authorized. Access to network services is given to students and staff who agree to act in a considerate and responsible manner. Signed parental permission is required for all students. All faculty and staff using the district's Internet access must sign a written contract.

All users are expected to abide by the generally accepted rules of Netiquette. These include, but are not limited to the following:

- Be polite. Do not be abusive or "bullying" in your messages to others.
- Use appropriate language.
- Do not assume that email is secure and/or confidential. Never send anything that you would hesitate to have viewed by others.
- Respect other people's privacy regarding mail and files. Do not reveal personal address or phone numbers, or those of students or colleagues.
- Keep paragraphs short and to the point. Be mindful of spelling.
- Check email regularly and delete unwanted messages as quickly as possible.

Prohibited activities include, but are not limited to the following:

- Using the network to transmit or retransmit copyrighted material (including plagiarism).
- Accessing, transmitting, or retransmitting threatening, harassing, bullying (cyberbullying) obscene and pornographic or trade secret material or any material deemed harmful to minors.
- Using the network to access, transmit or retransmit language that can be considered defamatory, abusive or offensive.
- Using social networking sites, chatting, or blogging unless associated with a specific curriculum related activity.
- Users of the BCSD network are forbidden to access, transmit, or retransmit information that could cause danger or disruption, engage them in personal, prejudicial or discriminatory attacks or that harasses or causes distress to another person.
- Users of the district network are forbidden to access transmit, or retransmit material that promotes violence or the destruction of persons or property by any device including but not limited to firearms, explosives, fireworks, smoke bombs, incendiary devices or other similar material.
- All users agree to report any accidental access of any of the material to the appropriate school authority so that the district can take steps to prevent similar future access.
- Using the network to download, upload or store large files such as music and video that are not related to projects or activities that are a part of the school curriculum.
- The use of flash (thumb) drives is limited to data storage only.
- No executable files of any type may be transferred to district property.

- Re-sending email chain letters or engaging in any spamming activities where bulk mailings of unsolicited email are sent.
- Damaging computers, computer systems, or computer networks (hardware or software). If a student maliciously damages BCSD technical equipment in such a way that requires service or repairs, the parent/guardian of the student is responsible for providing all expenses incurred for those services, grades K-12.
- Deliberate or careless action that damages the computer's configuration or limits the computer's usefulness to others.
- Downloading unauthorized software on school computers/networks. This includes students, teachers, staff and administrators. All software installed on district computers must be installed by the Technology Department and only after the prop- er licenses or authorizations for use have been acquired and verified.
- Creating, uploading, or transmitting computer viruses, worms or other disruptive software code.
- Making any attempt to defeat computer or network security on the district network or any other client, server, or network on the Internet. Hacking or attempting to gain access to unauthorized areas of the district network or the Internet is prohibited.
- Invading the privacy of other individuals. Using another person's password or account or providing his/her password to another person. Trespassing in another's folder, work or files, in the attempt to use others' work to "cheat" on assignments, tests, or any class work.
- Intentionally wasting limited resources.
- Using the network or school computer for unauthorized commercial, private, personal purposes or political lobbying.
- Unlawful activities
- Inappropriate sexual or other offensive content
- Any activity harmful to or reflecting negatively on the BCSD community or misrepresentation of BCSD, staff or students.

FILTERING

An Internet filter and firewall are in place on the BCSD network and district devices. This filter is a critical component of the BCSD network as well as Children's Internet Protection Act (CIPA) compliance since it allows valuable online Internet access while restricting access to specific unwanted material in the following categories:

- Pornography
- Gambling
- Illegal Drugs
- Online Merchandising
- Hate Speech
- Criminal Skills
- Alternative Journals
- Other Undesirable Materials

This filter is updated daily in order to restrict access to the above items. Filtering is not a 100% foolproof way of limiting access to appropriate sites. Inappropriate sites are added to the Internet daily. Students' activities are monitored while using the internet on the BCSD network. All inappropriate hits are logged along with the date/time and the IP address of the workstation making the request. Attempts to bypass the school Internet filters is in violation of this acceptable use policy and will be subject to disciplinary action that may include denial of access to technology, detention, suspension, expulsion, termination of employment or other remedies applicable under the school disciplinary policy, and state or federal law.

PRIVACY AND MONITORING

BCSD uses several methods to monitor and record network and internet activity both in real time and by review of stored data.

There is absolutely no expectation of privacy on the BCSD network. Activities at any workstation or transmission and receipt of data can be monitored at any time both electronically and by staff members. This includes the transmission and receipt of email, email attachments, Web browsing and any other use of the network.

Network administrators may review network storage files and communications to maintain system integrity

and ensure that users are using the system responsibility. While user files will not be examined without good cause, users should not expect that files stored on school computers will always be private. BCSD will fully cooperate with local, state or federal officials in any investigation related to illegal activities conducted through any BCSD Internet account or using BCSD technology.

SAFETY

- Students will tell their teachers or other school employee about any message they receive that is inappropriate or makes them feel uncomfortable.
- Students are responsible for the use of their individual accounts and should take all reasonable precautions to prevent others from being able to use their account.
- Under no conditions should a user provide his or her password to another person.

DISTRICT PROVIDED LAPTOP, TABLET, OR OTHER TECHNOLOGY DEVICE

TERMS: All users of district provided laptops, tablets, or other personal computing devices will always comply with the Benton County School District (BCSD) technology policies. Any failure to comply may result in termination of user rights of possession effective immediately and the district may repossess the device. Any lost, stolen and damaged devices must be reported to school authorities immediately.

TITLE: The district has legal title to the property. The user's right of possession and use is limited to and conditioned upon full and complete compliance with this agreement and all district policies and procedures. Any device or equipment must be returned to the district upon demand of administration or at the end of the school term.

Routine use guidelines.

- Only use your school email address for communication on district devices.
- School-approved games are allowed only when teachers have given permission to play.
- Do not ever carry, lift, grab, or hold any electronic device by the screen, except for tablets.
- When moving between classrooms, close the lid completely and place the electronic device in your bag or carry with both hands.
- Never throw, slide, or drop your electronic device.
- No food or drinks are allowed near electronic devices.
- Sign out of your electronic device when left unattended.
- Do not allow anyone to use your account or device unless authorized.
- Keep all passwords and login info private.
- Do not install or load any unauthorized software on district devices.
- Use of electronic devices on thick cloth (blankets, towels, etc.) will cause the device to overheat and is not permitted.
- Do not leave any electronic device in a location where it can be damaged by excessive weight (being sat on or laid on, heavy object on top, etc.) or knocked off or dropped from any surface (sofa, chair, table, etc.)

LOSS, THEFT OR FULL DAMAGE:

If a device is stolen, the employee or parent/guardian (in the case of a student) must immediately notify the school administration. At that time, the user or the parent/guardian will be required to file a police report. Once a police report has been filed, the district, in conjunction with the local law enforcement agency may deploy locating software to aid authorities in recovering the device. It is imperative that a lost or stolen device be reported immediately. If the stolen device is not reported within three calendar days to a district/school administrator, the employee or parent/guardian will be responsible for full replacement cost.

If a device is lost or damaged as a result of irresponsible behavior, the user or the parent/guardian will be responsible for the full replacement or repair cost plus a fee of $25.

Device replacement costs are as follows:

Laptop/Computer	$900
Chromebook	$350
Charger	$35
Case	$80
Tablet/iPad	$350

Replacement cost of devices not listed above will be determined by school administration at the time of the loss.

Students or employees who leave the district during the school year must return all devices and additional accessories to the school administrator. Users who do not return devices are subject to wage garnishment, withholding of school records, or enforcement with law enforcement.

CONSEQUENCES OF POLICY NON-COMPLIANCE

Violation of this TAUP (Acceptable Use Policy) may result in the denial, suspension or cancellation of the users' privileges as well as other disciplinary and/or legal action deemed appropriate and imposed by the school administration, district administration and/or local, state or federal law enforcement officials. Other action not specified above may include but are not limited to monetary restitution, school suspension or expulsion, detention or any other action deemed appropriate by the administrative authorities. Reinstatement procedures will be individually addressed. Any disciplinary action that is a result of an alleged violation of this policy can be appealed through the normal channels provided by the disciplinary policy of the BCSD.

Signatures on the TAUP agreement are legally binding and indicate the parties who have signed (parent/guardian) have read the terms and conditions carefully and understand their significance.

Due to the rapidly changing technology environment, BCSD reserves the right to determine if an action not listed in this document is inappropriate, and the students may be subject to discipline.