

BYOT



**Bring Your Own Technology
2014-2015**

Blount County Schools

**Student, Teacher and Parent Guide and
Acceptable Use, Media Release, and Internet
Safety Procedures**

Table of Contents

I.	General Information.....	3
II.	Purpose	3
III.	School Liability Statement	3
IV.	Expectations for Use	3
V.	Plan	5
VI.	Responsible Student Use of Personally Owned Devices.....	5
VII.	Frequently Asked Questions.....	6
	a. Students.....	6
	b. Staff.....	8
	c. Parents	9
VIII.	BYOT Acceptable Use	10
IX.	Acceptance Use, Media Release, and Internet Safety Procedures	11
X.	Acceptance of Terms and Conditions (Students.....	17
XI.	Acceptance of Terms and Conditions (Employees)	18

General Information

Access to the BCS Guest Network, whether with school-provided or personal devices, is filtered in compliance with the Children’s Internet Protection Act (CIPA). However, access from personal devices is limited to internet use only. Students will not have access to any documents that reside on the school network from their personal devices.

Access to the BCS Guest Network is a privilege, not a right. Any use of the wireless network entails personal responsibility and compliance with all school rules. The use of the BCS Guest Network also allows IT staff to conduct investigations regarding inappropriate internet use at any time, by administrator request.

Purpose

The Blount County Schools’ mission is to maximize the academic potential of every child in a safe and personalized environment. Goal #4 of the strategic plan states that Blount County Schools will graduate students who are college and career ready and prepared for post-secondary, education, careers and citizenship.

School Liability Statement

Students bring their personal technology devices to use at Blount County Schools at their own risk. It is their duty to be responsible for the upkeep and protection of their devices. BCS is in no way responsible for personal devices that are broken, lost or stolen while at school or school-sponsored activities nor is BCS responsible for the maintenance or upkeep of any device (keeping it charged, installing updates, or fixing any software or hardware issues).

Expectations for Use

- Use of personal devices during the school day is at the discretion of teachers and staff. Students must use devices as directed by their teacher.
- Students will only use appropriate educational application on their devices (i.e., no games and/or non-school related tasks or functions).
 - Examples of an unacceptable device in this policy shall include but are not limited to gaming devices or consoles, laser pointers, modems or routers, and televisions.
- Primary use of the personal device at school is educational. Personal use is secondary.
- The use of a personal device is not to be a distraction in any way to teachers or students. Personal devices must not disrupt class in any way.
- Students are not to call, text message, email, or electronically communicate with others from their personal device, including other students, parents, guardians, friends, and family

during the school day unless directed by their teacher or during designated times (i.e., lunch).

- The use of personal devices falls under BCS Acceptable Use Policy.
- Students are permitted to access only the school's network through their personal devices, not private networks.
 - Personally owned devices used in school are not permitted to connect to the Internet through a 3G, 4G, or other content service providers. Personally owned devices should access the Internet via Blount County Schools' content filtered wireless network.
- Students shall make no attempts to circumvent the school's network security and/or filtering policies. This includes setting up proxies and downloading programs to bypass security.
- Students shall not distribute pictures or video of students or staff without permission (distribution can be as small as emailing/texting to one other person or as large as posting image or video online).
- If a student is told to stop sending communications, that student must cease the activity immediately.
- Use of personally owned devices is permitted during instructional time for educational purposes only.
- Blount County Schools shall not be liable for the loss, damage, misuse, or theft of any personally owned device brought to school.
- Blount County Schools reserves the right to monitor, inspect, copy, and review a personally owned device or file when administration has a reasonable suspicion that a violation has occurred.
- Student must be aware of appropriateness of communications when using district or personally owned devices. Inappropriate communication is prohibited in any public messages, private messages, and material posted online by students. Students may not utilize any technology to harass, threaten, demean, humiliate, intimidate, embarrass, or annoy their classmates or others in their community. This is unacceptable student behavior known as cyber-bullying and will not be tolerated. Any cyber-bullying that is determined to disrupt the safety and/or well-being of the school is subject to disciplinary and/or legal action.
- Use of personally owned devices in locker rooms, restrooms, and nurses offices is expressly prohibited.

- Students are not permitted to use any electronic device to record audio or video media or take pictures of any student or staff member without their permission. The distribution of any unauthorized media may result in discipline including but not limited to suspension, criminal charges, and expulsion.
- All students shall review this policy yearly and sign (along with parent/guardian signature) the Acceptable Use, Media Release, and Internet Safety Procedures. Blount County Schools reserves the right to restrict student use of district owned technologies and personally owned devices on school property or at school-sponsored events.

Plan

Students in grades 3-12 may bring their own technology tools to their school campus. Students will be expected to access the internet through the BCS Guest Network, which will be available in every building in the district. All students will have signed the BCS Acceptable Use, Media Release and Internet Safety Procedures, which requires that they use the BCS guest login to access the internet. Users will be prompted to accept the following terms of use prior to each attempt at connecting to the BCS guest network:

BCE is providing wireless connectivity as a guest service and offers no guarantees that any use of the wireless connection is in any way secure, or that any privacy can be protected when using this wireless connection. Use of the BCS wireless network is entirely at the risk of the user, and BCS is not responsible for any loss of any information that may arise from the use of the wireless connection, or for any loss, injury or damages resulting from the use of the wireless connection. By entering, "Accept" below, you are agreeing to all cautions and policies as they pertain to non-district devices.

Students, staff, or visitors who do not accept the terms of service, will not be able to access the BCS Guest Network. The terms of service prompt will post each time an outside user attempts to use this network. Once on the guest network, all users will have filtered internet access just as they would on a district owned device. The BCS Guest Network is filtered in accordance with the Children's Internet Protection Act (CIPA). All teacher users will be filtered at the student level when using personal technology devices.

Responsible Student Use of Personally Owned Devices

The Blount County Board of Education developed this policy in order to maintain a safe and secure environment for students and employees.

A personally owned device shall include 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. Examples of personally owned devices include but are not limited to: MP3 players and iPods; iPads, Nooks, Kindle and other tablets; laptop and netbook computers; personal digital assistants (PDAs); cell phones and smart phones as well as any device with similar capabilities.

Educational purposes include classroom activities; career development, communication with experts, homework and limited high quality self-discovery activities. Students are expected to act responsibly and thoughtfully when using technology resources. Students bear the burden of responsibility to inquire with school administrators and/or teachers when they are unsure of the permissibility of a particular use of technology prior to engaging in the use.

Frequently Asked Questions

Students

I have turned in my signed copy of the BCS Acceptable Use, Media Release and Internet Safety Procedures. Can I start bringing my device to school?

Answer: Yes, by signing the BCS Acceptable Use, Media Release and Internet Safety Procedures you have secured permission to participate in BYOT.

I have my laptop with me in class. How do I get on the internet now?

Answer: Most laptops or other personal devices will detect a wireless connection when you are near one. Most of the time your technology device will ask you if you would like to join the network. When prompted, choose BCS Guest from the list. Once you choose this network, you will be prompted to accept the terms of service. Read this carefully, so that you will know what should be expected.

My laptop is not prompting me to choose a wireless network. Is there another way to connect?

Answer: In the settings menu of your device, there is usually an icon for a network. Go to this icon and choose "BCS Guest" form the list or prompt your computer to look for wireless networks in range. Always consult your device's owner's manual or other available support for exact directions to access a wireless network.

I brought my iPad to school to use in the classroom, but my teacher said I couldn't use it in her classroom. Can I still use it?

Answer: The classroom teacher has the final say on procedures in the classroom. If he or she asks you not to use your technology at a particular time, then you must follow those directions.

I just can't get my laptop to connect to the network. Can I get some help from someone?

Answer: Check your owner's manual or other support resources for issues concerning connectivity. Frequently peers will have similar devices and will be able to support each other. Classroom time will be focused on instruction, so your teacher will not be able to help you. BYOT participants will need to test their ability to connect to the network outside of instructional time.

I need to save my work to the BCS network. Why can't I access this resource?

Answer: You are on the Guest Network. It is not the same as the network you would normally access from a campus computer. You will not see your shared folder, so you will need to save your work in another place. Some options include a flash drive or your own hard drive.

I need to print the spreadsheet I just created, why is there no printer listed when I try this?

Answer: Printers will not be available when you login to the guest network. Some printing solutions include emailing the document to your teacher to print, save it to a flash drive and print it from home or another classroom computer. Keep in mind that using campus printers in the classroom or other learning spaces is at the discretion of the teacher administrator.

My device was stolen when I brought it to school. Who should I contact about this?

Answer: Bringing your own technology tools 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 in case of theft. BCS is not responsible for the theft of a device nor are we responsible for any damage done to the device while at school. Any time a theft occurs, you should contact a school administrator to make him/her aware of the offense.

Why am I filtered on my own computer? Shouldn't I be able to see what I want to on my own device?

Answer: Student filtering is a requirement of all public schools. The Children's 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. The network you are using while at school belongs to BCS and will be filtered.

I have a data plan from a provider (AT&T, SPRINT, Verizon, etc...) on my digital device that allows internet access without using the BCS guest access. Is this allowable?

Answer: Students are expected to follow the submitted acceptable use procedures when accessing the internet through any device. All students are expected to use the BCS guest login to access the internet. Students should not access the internet through any cellular data provider while on campus. Students that do not follow the guidelines may lose the privilege of using a device at school.

Am I still held accountable for the acceptable use agreement I signed at the beginning of the school year even through this is my own personal computer?

Answer: Yes. The acceptable use agreement for BCS remains in effect even when you are using your own laptop, smart phone, iPad, etc... Each time you attempt to access the network at school you will be prompted to accept the terms of service. Violating the terms of the guidelines would be a student code of conduct violation and would be dealt with on the campus with the school administrator.

Staff

My classroom is not conducive to student owned technology. Am I required to allow my students to access their technology tools in the classroom?

Answer: BCS encourages teachers to leverage student owned technology tools in their classroom for learning and the needs of the student. The design of the lesson should be used to determine the best use of student provided technology and the rules that apply. Student needs may also determine the use of the device. For example, a student may use the device for note taking to support their personal learning while in the classroom.

Some of my students cannot access the network on their laptops or phones. I don't have time in a class period to help them with this. Should I contact the building level technology coordinator or call the technology department?

Answer: No. Students who cannot access the BCS guest network or who may have technical issues with their technology tool need to take care of this issue by working with their user's manual or other available support that came with the device. These are not BCS devices and the district is not allocating additional resources at this time to troubleshoot issues. You are welcome to help if you choose, but it is not a staff member's responsibility to ensure that student owned technology is functioning properly.

I have students and staff on my campus who are accessing the internet using their provider's data plan (AT&T, Sprint, Verizon, etc...) on their smart phones or laptops, hence bypassing the filter. Is this allowable?

Answer: Students are expected to follow the submitted acceptable use agreement when accessing the internet through any device. Teachers should monitor the use of devices by students.

I have my own laptop and a smart phone. I would like to utilize these tools at work. Does this new plan include school staff?

Answer: Yes. Campus staff can also access the guest network. Keep in mind that the guest network is going to be filtered at the student level for everyone accessing it. School printers will not be accessible with your own devices as well.

One of my students was using his laptop to bully another student at school. How do I handle this?

Answer: Any disciplinary infractions that occur from using technology tools should be referred to an administrator. This would be a student disciplinary issue.

Will students have access to any common software packages via the guest network access?

Answer: No locally installed software packages will be available but all web based resources provided by the county will be accessible to the students.

What shall I do if one of my student's devices is damaged or stolen?

Answer: Any theft issues should be handled as you normally would at school. BCS is not responsible for any damage or theft of student owned technology tools. It would be good to remind students to keep a record of the device's serial number just in case a theft occurs. Staff members are encouraged to practice reasonable precautions such as locking empty classrooms when devices are left there.

Parents

My son is bringing his iPad to school for instructional purposes. Will he have access to things he normally does with district equipment?

Answer: Your son will have access to any of the web based software schools currently use (databases, library search tools, etc...). Software may run differently on different devices for varying reasons. You should consult your owner's manual or other support materials provided with the device for software limitations. (Example – iPads cannot run software requiring Flash Player).

As a parent, am I required to add additional software (virus protection, filter, tracking device, etc...) to my child's technology tool?

Answer: No. Currently we are not requiring any additional software for school use. Virus protection is always advised, but not required. While on the BCS guest network, students will be monitored through the district's filter, so there is no need for additional filtering software.

I have read the terms of service and I do not wish to have my daughter accessing the internet using her own laptop. Is this allowable in this plan?

Answer: Your daughter is not required to bring a device to school. Your daughter would still need to submit the BCS Acceptable use, Media Release and Internet Safety Procedures to use district owned devices. The school will provide, whenever possible, a district owned device for use within the class period as needed for instructional purposes at the discretion of the teacher.

I am the president of a booster club at my child's school. We hold meetings at night. Will we have access to the BCS guest network after school hours for our meetings?

Answer: Yes. The guest network will be accessible after school hours.

If my daughter's laptop is stolen or damaged, what recourse can I take?

Answer: The district is not responsible for any damage or theft of student owned equipment. Keeping track of the device's serial number, model and type at home is suggested. Theft or vandalism of any kind should be reported immediately to a campus administrator so he/she can take the appropriate steps.

What are the school/classroom rules for using student owned devices including phones?

Answer: Teachers make the final decision for any tools used in the classroom; student owned equipment would be no different. It will be up to the individual teachers to communicate their expectations to parents and students. For example, the student may choose to use their personal device for note taking. During class the teacher may ask the student to turn off the device during a test. Contact your child's teachers or school for expectations.

Will my child have access to communication tools like email or message boards while on the BCS guest network?

Answer: Students will have access to outside email accounts (Yahoo, Google, etc...) but will not have access to message boards.

Where can I see the Acceptable Use Policy for Technology?

Answer: Board policy is available online at the following link:

<http://boardpolicy.net/documents/detail.asp?iFile=16019&iType=4&iBoard=79>.

BYOT Acceptable Use

Participants are expected to return a signed BCS Acceptable Use, Media Release and Internet Safety Procedures prior to bringing a personal device to school. Parent and student signatures acknowledge acceptance of the BYOT procedures.

BCS ACCEPTABLE USE, MEDIA RELEASE, AND INTERNET SAFETY PROCEDURES

PURPOSE

Blount County Schools provides student and employee access to the Internet as a means to increase learning and productivity toward achieving 21st century literacy. The purpose of this contract is to assure that users recognize the procedures which the school imposes on their use of Internet, electronic media resources, and release of student information. In addition, this contract requires that users agree to abide by the BCS Board of Education policies, the BCS Computer Guidelines, and stipulations of the Children's Online Privacy Protection Act 47 USC Section 231 (COPPA), the Family Education Rights and Privacy Act (FERPA), and the Children's Internet Protection Act (CIPA) as well as laws pertaining to stalking and harassment. The policy is promulgated so as to be in compliance with the public records laws of the State of Tennessee.

THE CONTRACT

BCS has outlined the following guidelines as required for all technology users. The district has taken measures designed to protect students and adults from obscene information and restrict access to materials that are harmful to minors. Failure to follow all or part of these guidelines, or any action that may expose BCS to risks of unauthorized access to data, disclosure of information, legal liability, potential system failure, or compromise the safety of users is prohibited and may result in disciplinary action up to and including loss of network privileges, confiscation of computer equipment, suspension, termination of employment and/or criminal prosecution.

1. Employee Compliance

All employees must comply with the Blount County Board of Education policies

Any employee receiving a mobile device (i.e. laptop, tablet) from the District must sign the Mobile Technology agreement at the time the device is issued (check out) and again when the device is returned (check in). All personnel with issued laptops must comply with BCS Laptop Procedures. Any employee receiving an electronic tablet from the District must comply with BCS procedures governing such electronic devices.

2. Student Compliance

All students must comply with the Blount County Board of Education policy 4.406, the Internet, Network Access, Computer Hardware policy.

Students who wish to have their photographs, names, or work posted on the BCS website or other publications and media must first receive consent by obtaining a parent or legal guardian signature on the Acceptable Use, Media Release, and Internet Safety.

Students shall report to school personnel any personnel electronically transmitted attacks in any form made by other over the Internet or local network using any BCS technology. Students shall understand information obtained via the Internet may or may not be correct.

3. Internet Safety

All students will participate in Internet safety instruction integrated into the district's instructional program in grades K-12. Internet safety professional development will be available to all teachers and administrators. Outreach programs to families and community will be offered annually. Schools will use existing avenues of communication to inform parents about Internet safety. The district Internet safety policy will be reviewed annually.

4. Student Participation in Bring Your Own Technology (BYOT) Program.

As new technologies continue to change the world in which we live, they also provide many new and positive education benefits for classroom instruction. Students in grades 3-12 may bring their own technology to campuses subject to the terms below:

a. Definition of Technology

For purposes of BYOT, "Technology" means personally owned wireless portable electronic equipment used for instructional purposes. All approved devices must allow access to the Internet through a fully functional web browser and be capable of accessing the BCS guest network. Recognizing the rapidly changing world of technology, the list of allowed devices will be reviewed annually. Approved devices include, smart phones, iPads, iPods, laptops, netbooks, tablet computers and eReaders that meet the definition of "technology."

b. Internet

All Internet access shall occur using the BCS guest network. Cellular network adapters are **not** permitted to be used by students to access the Internet at any time.

c. Security and Damages

Responsibility to keep privately owned devices secure rests with the individual owner. BCS, its employees and agents, are not liable for any device stolen or damaged on campus. If a device is stolen or damaged, it will be handled through the school administrative office in the same manner as other personal items that are impacted in similar situations.

d. Student Agreement

The use of personal technology to provide educational material is not a necessity but a privilege. A student does not have the right to use his or her laptop, cell phone or other electronic device while at school. When abused, privileges will be taken away. When respected, privileges will benefit the learning environment.

Students and parents/guardians participating in BYOT must adhere to all Board policies and the *BCS Acceptable Use, Media Release and Internet Safety Procedures*. Additionally:

- Students take full responsibility for personal digital devices at all times. The school is not responsible for the security of the device.
- The device must be in silent mode while on school campuses unless otherwise directed by the teacher.

- The device may not be used to cheat on assignments or tests or for non-instructional purposes during instructional time.
- The device may not be used to record, transmit or post photographic images or video of a person or persons on campus during school activities and/or hours unless assigned by the teacher as allowed by the *BCS Acceptable Use, Media Release and Internet Safety Procedures*.
- The device may only be used to access files or internet sites which are relevant to the classroom curriculum. Non-instructional games are not permitted.
- Students must comply with a teacher's request to turn off the device.

Students acknowledge and agree that:

- The school's network filters will be applied to the BCS guest network access to the internet and shall not be circumvented.
- The school district may collect and examine any device at any time for the purpose of enforcing the terms of this agreement, investigating student discipline issues, or for any other school-related purpose.
- Personal technology must be charged prior to bringing it to school, and the device must run off its own battery while at school.
- Students remain subject to all other school behavior rules.

5. Network Security

Only users with valid BCS network accounts are authorized to use the BCS network and computer equipment. Employees and students must only use their assigned network account. Employees and students are prohibited from giving anyone their network account information other than to authorized IT personnel.

No alternative network shall be created or used by any staff or student unless approved by the IT Department. "Alternative network" is defined as any wired or wireless network or sub-network located or accessible from any BCS property that is not part of the primary network managed by the IT Department. All network equipment must be installed and/or approved by IT Department staff.

Students may not allow another user access to use a computer while logged in. All computer users should always lock or logoff from the network before leaving their room or office.

For the protection and security of BCS data, all computers attached to the BCS physical network (a computer located at a BCS facility either wired or wireless), must be the property of BCS. A computer that is not property of BCS may not be attached to the network without first receiving approval from IT Department administrator.

Use of software designed to gain passwords or access beyond the rights assigned to a user or computer is strictly prohibited. Use of such programs risks the security of the network and is considered "hacking." Such unauthorized access is a violation of State and Federal law. Violators will be prosecuted. Should an employee or student inadvertently discover passwords or any other measure used to obtain unauthorized access, they must report it to the IT Department.

No user shall encrypt files or folders or attempt to hide files or folders stored on a network server or local workstation unless approved by the IT Department administrator.

All network users may be monitored at any time by authorized personnel for the purpose and inspection of compliance to these guidelines.

6. Workstation/Computer Use

All employees and students are prohibited from installing any software on any computer unless authorized in writing by a member of the IT Department. Illegal downloads or use of copyrighted software, music, videos, pictures or other files is strictly prohibited. Only compatible, legitimate and approved school related software is acceptable.

All employees and students are prohibited from using any BCS computer for illegal, obscene, pornographic, personal profit or commercial activity.

Changing or tampering with any computer's system configuration is strictly prohibited.

Any attempt to bypass the internet content filtering by use of a proxy or other means is strictly prohibited unless authorized by the IT Department. Content is filtered for all users accessing the Internet through the BCS network. Content is filtered for all users accessing the Internet through the BCS network.

Any desktop applications designed to limit access to students or staff, other than those used by the IT Department for network security purposes, is prohibited.

Use of a broadcast messenger service such as "net send" to send messages over the network is prohibited except in the case of an emergency. Permission should be obtained from the Director of Schools or the Technology Supervisor before anyone sends a system-wide email to blountk12.

Computers found to be tampered with or computers with unapproved software or files will be re-formatted and restored to compliance.

No computer shall be moved by anyone other than IT Department personnel unless approved by a member of the IT Department.

7. Server Software

Only authorized IT Department personnel will install software to the server.

8. Saving Documents

Employees and students must save all documents to the network but shall not save any applications to the network without authorized described herein below. Due to server storage limitations, any applications or executables residing in a user directory will be deleted. (Exception is given where individuals have created applications as part of a curriculum assignment and such activity has been approved by a member of the IT Department).

9. Network Drives/Shares

Network drives have been provided to all users for the ease of use of network resources. Drive letters assigned to an authorized network user are specific to that individual user. Any attempt to gain access to a drive that is not assigned to a user is strictly prohibited.

All users have access to a Public directory on the server. This is the "W" drive. Please use it with caution as anyone can read and possibly delete information in this directory. Each user is to make sure a backup is created of anything placed in this directory. The IT Department will not restore anything deleted from the "W" drive.

10. Viruses and Virus Protection

The BCS IT Department will provide all virus protection and related software for all workstations and servers. Virus protection and related software will be installed by authorized IT personnel unless otherwise approved by the IT Department.

Do not open any email attachments from any unknown sender. Never send an email suspected of containing a virus. The intentional spreading of messages or files containing damaging or destructive programs or data is against federal law. Violators will be prosecuted. Contact the IT Department immediately to report a computer that may contain a virus.

There are many virus hoaxes. Never delete system files from a computer in order to remove a potential virus without first checking with the IT Department to make sure the virus is valid and not a hoax.

No student or employee is allowed remote access (access from outside the BCS network) to any BCS network resource from a non-BCS computer without first obtaining a working and updated virus protection program. This includes, but is not limited to, VPN Access and Webmail. Recommended virus protection programs include Microsoft, Sophos, AVG, Trend Micro, McAfee and Symantec.

11. Copyright Policy

All students and employees will comply with all applicable copyright laws in the use of all media and materials. All employees will model legal and ethical practice related to technology use as established in Blount County Board of Education policy 4.404.

12. E-mail

The BCS e-mail system has been provided for the internal and external communication of employees and board members. The e-mail system may not be used for personal gain or political or religious views or in any illegal, offensive or unethical manner. The e-mail system is intended only for valid and legitimate BCS related communication.

BCS does reserve the right to access any e-mail for any business purpose, and also for inspection for disciplinary or legal action.

Students are not provided with e-mail accounts at this time.

13. Electronic Communication

All communication conducted electronically between a BCS employee and a student shall be for the purpose of official business of the BCS system. BCS employees may only initiate texts to students with the permission of the parent/guardian.

E-mail communication from a BCS employee to a student shall only be through the teacher's BCS e-mail account.

14. Donations

The current minimum standard for all donated computers (either PC or Mac) are Intel Pentium 1.8GHz Core 2 Duo or above with 40 GB hard drive and 4 GB RAM. Regardless of the intended use of the donated computer, all donations must comply with this minimum and be approved by the IT Department. DO NOT ACCEPT A DONATION WITHOUT FIRST GAINING APPROVAL BY THE IT DEPARTMENT.

15. Mobile Device Expectations

Staff members may be issued a mobile device for official school use. Students may be allowed to use laptops during the school day at the discretion of the principal and/or teacher. The following procedures should be followed when using mobile devices:

- a. Mobile devices provided to staff and students belong to Blount County Schools. The user is responsible for the care of the device while it is being used.
- b. Mobile devices should only be connected to the Blount County Schools network.
- c. Users should not change settings and/or make any additions or changes to the mobile device in any way.
- d. Mobile devices should only be used for school use.

BCS ACCEPTANCE OF TERMS AND CONDITIONS - STUDENTS

These terms and conditions reflect the entire agreement of the parties and supersede all prior oral and written agreements and understandings of the parties.

If you are under the age of 18, a parent or guardian must also read and sign this contract.

I understand that should I fail to honor all the terms of this agreement, future Internet and other electronic media accessibility may be denied, including loss of the privilege of bringing an electronic device to school, and the school administration will consider it a major disciplinary infraction.

Student Name (Please Print)

Student Signature

Date

I have read this agreement and understand that the school wished to expand the availability of information to students and at the same time attempt to assure the appropriateness of this information as it relates to the goals of the school. By signing below, I give permission for the school to allow my son/daughter to have access to the Internet and other technology resources under the conditions set forth above.

Parent/Guardian Name (Please Print)

Parent or Guardian Signature

Date

I agree to the following release of information regarding my child:

The school or school district may feature my child in the broadcast and print media, on the school or school district website, and in district publications and programs.

Parent/Guardian Name (Please Print)

Parent or Guardian Signature

Date

Student Name (Please Print)

BCS ACCEPTANCE OF TERMS AND CONDITIONS - EMPLOYEES

These terms and conditions reflect the entire agreement of the parties and supersede all prior oral and written agreements and understandings of the parties.

I understand that should I fail to honor all the terms of this agreement, future Internet and other electronic media accessibility may be denied, and the school administration will consider it a major disciplinary offense.

Employee Name (Please Print)

Employee Signature

Date

MOBILE DEVICE AGREEMENT

I understand that should I be assigned a mobile device, it is property of Blount County Schools and should be used for official school use only. Failure to comply with the procedures and expectations for mobile device use will result in the loss of the device and could result in further disciplinary action. I also understand that I will be responsible for any damage incurred to the mobile device beyond normal use.

Employee Name (Please Print)

Employee Signature

Date