Brown County Schools
Acceptable Use Guidelines for Technology Services

Technology is an integral part of a student's educational experience and must be used in support of the educational objectives of Brown County Schools (BCS). All students are expected to use technology and the Internet in an appropriate manner. Students are required to bring a fully charged computer (tablet) to school daily as well as electronic media, and or files required for class.

Technology includes, but is not limited to, computers, other hardware, electronic devices, software, Internet, e-mail, all other networks, etc. Students are responsible for appropriate use of all computers to which they have access. Obscene, pornographic, threatening, or other inappropriate use of any technology and use of hardware and/or software which disrupts or interferes with the safety and welfare of the school community, is prohibited, even if such uses take place off school property (i.e., home, business, private property, etc.). Altering the pre-set BCS software image is prohibited. **Brown County Schools adheres to the provisions of the Children's Internet Protection Act (CIPA).**

I. **General Terms and Conditions of Use**
   A. Brown County Schools provides all students access to the Internet and also, in some cases, an issued electronic device, as a means to enhance their education. There are limitations imposed on student use of technology and Internet resources, which are included herein.
   B. The *BCS Acceptable Use Agreement for Devices* and the *BCS Standards for Proper Device Care* must be followed in addition to this document.
   C. Transmission of any material in violation of Federal, State, or local law, ordinance, School Board policy, regulation or the Code of Student Conduct is prohibited. This includes, but is not limited to, the following: copyrighted material, cyber bullying, inappropriate use of blogs and/or wiki pages, threatening, violent, obscene, or pornographic communication and/or material, material protected by trade secret, and uploaded or created computer viruses.
   D. To protect students while at school and home, and to meet the Children's Internet Protection Act (CIPA) requirements, access to the Internet is filtered through a commercial filtering system.
   E. Use of technology for commercial activities is prohibited unless explicitly permitted by the School Board. Commercial activity includes, but is not limited to, the following:
      1. any activity that requires an exchange of money and/or credit card numbers;
      2. any activity that requires entry into an area of service for which the school will be charged a fee;
      3. any purchase or sale of any kind;
      4. any use for product advertisement or political lobbying.

II. Acceptable Use and Internet Safety Policy (in accordance with Children's Internet Protection Act (CIPA). The following rules are in effect for all Brown County Schools' computers unless otherwise directed by a teacher or administrator:
   A. It is the responsibility of each student that student-loaded files and programs do not consume hard drive space needed for instructional or educational requirements.
   B. Teachers may authorize students to use Internet communication that includes filtered e-mail, discussion boards and chat rooms, for instructional purposes only.
   C. Downloading, uploading, importing music and videos are allowed outside of school hours, so long as it does not violate copyright law or contain words or images that are pornographic, obscene, graphically violent or vulgar.
   D. File sharing must be approved and directed by the teacher.
   E. Headphones may be used during the instructional day with teacher permission as long as the use does not

interfere with the instructional program.

F. Upon request by an administrator or teacher, students should make messages or files, either sent or received, available for inspection.

III. Prohibited Acts

A. Students are prohibited from accessing or attempting to access instant messages, chat rooms, forums, e-mail, message boards, or hosting personal web pages during the instructional day unless authorized by a teacher or administrator for instructional purposes.

B. Students are prohibited from using proxies to bypass Internet filters.

C. Students shall not attempt to locate or make use of files that are unacceptable in a school setting. This includes, but is not limited to pornographic, obscene, graphically violent or vulgar images, sounds, music, video, language, or materials, including screensavers, backdrops, and/or pictures.

D. Students shall not download, upload, or import games, screen animations, or programs or files that can be run or launched as a stand-alone program. These programs or files are sometimes known as "executable files."

E. Illegal use or transfer of copyrighted materials to a school owned computer, including laptops, is prohibited. Students should only download/import music or materials (files) that they are authorized or legally permitted to reproduce, or for which they have the copyright.

F. Students are prohibited from playing games during the instructional day unless otherwise directed by a teacher or administrator.

G. Students are not allowed to connect a laptop to Ethernet jacks in the school unless instructed by the teacher or administrator.

H. Additions, modifications or deletion of files, except in the student's 'directory' or 'home directory,' are prohibited.

I. Students shall not save, transfer or load non-school related material on a school file server.

J. USB storage devices can only be used for file storage and shall not be used to launch software.

K. Students are prohibited from creating or using unauthorized networks including, but not limited to, voice, data, IP, peer to peer, or proxy networks.

IV. Personal Responsibility and Integrity. All students are expected to behave responsibly and with integrity when using technology. These responsibilities include, but are not limited to, the following:

A. All who use BCS technology resources must recognize that the work of all users is valuable; therefore, every user must respect the privacy of others. Users shall not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent or assume the identity of other users.

B. Students shall not reveal unauthorized personal information about themselves or others.

C. Students shall not share passwords with one another for any reason and should make every effort to keep all passwords secure and private.

D. Students shall use his or her real name in all educational activities that incorporate technology or the Internet (e.g., distance learning, online distance learning, etc.). Students shall use their full names in school sanctioned discussion boards or e-mails and follow proper grammatical rules. Students shall not use Internet slang, such as "lol" or "bff" to disguise or otherwise mask inappropriate communication, and shall refrain from typing in all capital letters, which indicates yelling or bullying of the recipient, when communicating in this forum.

E. Students should understand when communicating electronically that their screen name, posted photographs and language represents them online and must meet acceptable use standards.

F. Students should use technology for school-related purposes only during the instructional day.

G. Students should use the resources available through the Internet and other electronic media to supplement material available through the classroom, media center or through any other resource provided by the school.
H. Students are expected to maintain their instructional files and media in a responsible manner, which includes backing up at regular intervals.
I. Students should not copy, change, read or use files in another user's storage area (such as hard disk space, disks, mail, server space, personal folders, etc.) without the user's permission.
J. Students should not participate in cyber bullying: the act of making personal attacks or threats against anyone using this resource. Students should report to a teacher or administrator any personal electronically transmitted attacks in any form made by others over the Internet or Local Area Network (LAN).
K. Students shall respect the privacy of others. Students should re-post (to make appear online again) communications only after obtaining the original author's prior consent.
L. Students shall not deface the laptops in any way. This includes, but is not limited to, marking, painting, and drawing, marring, or placing stickers on any surface of the laptop.
M. Students shall not knowingly introduce or knowingly allow the introduction of any computer virus to any BCS computer.

V. Security. Security on any computer system is a high priority. Remote monitoring of students' BCS-issued technology to determine appropriate use during the instructional day will occur at each school site. Students are required to report any security problem to a teacher or administrator. To maintain a safe and secure technology environment, the following actions are prohibited:

A. Attempting to log on to the BCS network using another's identity
B. Bypassing or attempting to bypass BCS filtering, security and/or monitoring software
C. Attempting to conceal the identity of one's computer or user information on the BCS Network
D. Connecting a personal, non-school-district-owned desktop computer, laptop computer, wireless personal digital assistant (PDA), smart phone or any other network (wireless or directly plugged) device to any part of the BCS network (local area network "LAN", wide area network "WAN", or metropolitan area network "MAN".)
E. Creating or using unauthorized networks, including, but not limited to, voice, data, IP, peer-to-peer or proxy networks.
F. Using BCS equipment for any illegal activity
G. Downloading, uploading, importing or viewing files or websites that promote the use of illegal drugs, alcohol, pornography, or illegal and/or violent behavior
H. Tampering with computer hardware or software, unauthorized entry into computers, and vandalism or destruction of any computer or files

VI. Privacy/Copyright. The illegal use, distribution or transfer of copyrighted material on BCS computers is prohibited.

VII. Alteration of Pre-set Software Image. Altering/modifying the original BCS pre-set software image is prohibited. Examples include, but are not limited to, the following:

A. Loading/installing any software applications
B. Changing the computer name
C. Changing or removing operating system extensions
D. Altering security, filtering, and/or monitoring software
E. Altering the pre-loaded operating system or applications

F. Taking apart the computer for access to internal parts

G. Attempting to or changing the configuration of the software or hardware that controls access to the network and Internet; or any other electronic media which includes the use of proxies.

VIII. Disciplinary Consequences. Failure to honor all of the regulations listed above may result in disciplinary action. Possible actions include, but are not limited to, the following

A. Removal of unauthorized files and folders
B. Denial of Internet and other electronic media accessibility
C. Recall of the student's device
D. Revocation of Computer Access and Use
E. Student Conference
F. Parent Contact or Conference
G. Restitution
H. Community Service
I. Detention
J. Suspension
K. Recommendation for Expulsion
L. Violations of these regulations may also result in criminal charges if the violation of the regulation is also a violation of Federal, State, or local law or ordinance.