

Bartlett City Board of Education		1021
Descriptor Term: TECHNOLOGY USE AND INTERNET SAFETY	Descriptor Code: Board Operations	Issue Date: 2/27/2014
	Rescinds:	Revised: 12/17/2015 07/24/2025 07/23/2026

1 The Bartlett City Board of Education provides access to the Internet through a variety of
2 technology resources including, but not limited to, computers, tablets, cloud computing, and
3 storage solutions. The Board provides such access as an instructional and professional resource
4 and intends that students and staff benefit from these resources in a safe, legal, appropriate and
5 responsible manner.

6 The Board establishes this Policy to govern student and employee use of BCS technology
7 resources, to prevent unauthorized access and unlawful activities by users, to prevent
8 unauthorized disclosure of or access to sensitive information, and to comply with the Children's
9 Internet Protection Act (CIPA).

10 This Policy applies to all BCS technology resources including, but not limited to, BCS networks
11 and all devices connecting thereto. This Policy applies to all BCS-provided technology use,
12 whether on or off campus. BCS students, employees, volunteers, interns, and authorized
13 personnel using district-provided technology shall, at all times, comply with this Policy and its
14 accompanying procedures and are expected to be responsible for professional and appropriate
15 behaviors online and offline.

16 Before any student or employee is permitted use of the district's technology, including hardware,
17 software, intranet, internet, or email, and annually thereafter, such student or employee shall sign
18 a copy of the BCS Internet Safety and Acceptable Use of Technology Policy. All users of BCS
19 technology, including those who access the district's network for any purpose, agree to be bound
20 by the terms of this Policy and its accompanying procedures, even if no signed Agreement
21 remains on file.

22 CIPA Compliance and Internet Safety Measures¹

23 The Superintendent or his/her designee will develop and maintain administrative procedures for
24 the appropriate use of technology by staff and students. Internet safety measures will include but
25 not be limited to:

- 26 A. Controls for access by students to inappropriate matter on the Internet and the World Wide
- 27 Web
- 28 B. A safe and secure environment for students when using electronic mail, chat rooms, and
- 29 other forms of direct electronic communications.
- 30 C. Prevention of unauthorized access, including "hacking" and other unlawful activities on-
- 31 line
- 32 D. Prevention of unauthorized disclosure, use, and dissemination of student personal
- 33 information

¹ Children's Internet Protection Act (Public Law 106-554)

- 1 E. Use of technology to restrict students' Internet access to material that is obscene or
2 harmful to them

3 The Superintendent or his/her designee shall establish procedures to ensure the district's
4 education technology is not used for purposes prohibited by law. The process shall include but
5 not be limited to:

- 6 A. Utilizing technology to block or filter Internet access to material that is obscene or harmful
7 to students
8 B. Maintaining and securing a usage log
9 C. Monitoring on-line activities of students

10 The BCS Director of Technology shall take commercially reasonable steps to select technology
11 for BCS's computers having internet access that will, to the extent possible, satisfy the foregoing
12 process and filter, block, or otherwise prevent access to pornography or obscenity through online
13 resources and prohibit, and to the extent possible, prevent a user from sending, receiving,
14 viewing, or downloading materials that are deemed to be harmful to minors as defined in T.C.A.
15 §39-17-901.

16 Internet Safety Instruction²

17 Students will receive appropriate instruction in Internet safety and digital citizenship as a part of
18 any instruction using devices that provide access to the Internet. Internet safety instruction will
19 include, but not be limited to, appropriate online behavior, interaction with others while using social
20 networking websites or chat rooms, and cyberbullying awareness and response.

21 The Superintendent shall also provide adequate in-service instruction on internet safety.

22 Students, parents, and employees will be provided with material to raise awareness of the
23 dangers posed by the Internet and ways in which the Internet may be used safely. Parents of
24 students attending Bartlett City Schools shall also be provided with the district Acceptable Use of
25 Network and Electronic Media Agreement and accompanying guidelines for such Agreement. All
26 network users shall abide by all laws, the Acceptable Use Policy, and all district security policies
27 when using the district network or district owned devices.

28 Expectations and Acceptable Use of Network and Internet

29 The Superintendent or his/her designee shall develop an Internet Safety and Acceptable Use of
30 Technology Agreement and adopt guidelines for such Agreement that shall apply to all Bartlett
31 City Schools students, employees, volunteers, interns and contractor personnel, whose access
32 to, or use of, technology is provided by or through Bartlett City Schools.

- 33 A. All users shall act in a responsible, ethical, and lawful manner when using the BCS
34 information technology resources.
35 B. All users shall use technology resources in a manner that does not result in intentional
36 damage of school equipment, networks, stored data, or hosted cloud platforms or
37 systems.
38 C. Users shall secure technology resources against loss or theft and shall maintain
39 technology resources in good working order.
40 D. Users shall report a malfunctioning, damaged, lost, or stolen device immediately to the
41 BCS Technology department.
42 E. Users shall monitor all activity on their account(s) and report suspicious activities to BCS
43 Technology department immediately.

² T.C.A. §49-1-221

- F. Users shall refrain from plagiarizing works accessed through BCS technology resources. Plagiarism is taking the ideas or writings of others and/or using AI generated content and presenting them as if they were one's own works.
- G. Staff members who supervise students, control electronic equipment, or otherwise have occasion to observe student use of technology shall monitor the use of this equipment to assure that it conforms to the mission and goals of the district.
 - a. Parents/guardians wishing to deny independent access to BCS technology resources may do so by returning a signed right of refusal form supplied by the school. This document shall be kept on file as a legal, binding document. (In order to modify or rescind the agreement, the user's parent/guardian must provide the principal with a written request.)
- H. All users shall follow this policy.

Unacceptable Uses of the Network or Internet

Bartlett City Schools reserves the right to take immediate action regarding activities on its network that (1) create security and/or safety issues for the district, students, employees, schools, network or computer resources, or (2) other activities as determined by the district as inappropriate.

Prohibited activities include, but are not limited to, the following:³

- A. Illegally installing, transmitting, or otherwise violating copyrighted materials;
- B. Violating any state or federal law, municipal ordinance, or BCS Policy;
- C. Accessing, uploading, downloading, or sending materials that are offensive, profane, threatening, pornographic, obscene, harassing, demeaning, sexually explicit, confidential, or materials that encourage others to violate the law;
- D. Using BCS technology to engage in criminal activities that can be punished under law;
- E. Using BCS technology to sell or purchase illegal items or substances;
- F. Gaining unauthorized access to student or employee accounts, files, and/or data;
- G. Unauthorized sharing of credentials for any technological resource;
- H. Unauthorized photography, videos, or use of an individual's likeness without their knowledge and consent;
- I. Using BCS technology to impersonate another individual;
- J. Trespassing in another's folders, online accounts or systems, work, or files;
- K. Causing harm to others or damage to their property, such as:
 - a. Using profane, abusive language; threatening, harassing language, or making damaging or false statements about others or accessing, sending, or downloading offensive, harassing, or disparaging materials;
 - b. Deleting, copying, modifying, or forging other users' names, emails, files, or data; impersonating other users, or sending anonymous email;
 - c. Damaging computer equipment, files, data or the network in any way, including intentionally accessing, transmitting or downloading computer viruses or other harmful files or programs, or disrupting any computer system performance;
 - d. Using any District computer to pursue "hacking", internal or external to the District, or attempting to access information protected by privacy laws;
- L. Using the network or Internet for commercial purposes, such as:
 - a. For personal financial gain;
 - b. For personal advertising, promotion; or
 - c. Conducting for-profit business activities and/or engaging in non-government related fundraising or public relations activities such as solicitation for religious purposes, lobbying for personal political purposes
- M. Bypassing any BCS filter through a web proxy, tethering, or any other means;

³ T.C.A. §39-14-602

- 1 N. Students are prohibited from accessing social media platforms, message boards, and/or
2 instant messaging services using the internet access provided by BCS, except when
3 expressly authorized by their teacher for educational purposes only.⁴
4 a. "Social media" is defined as a form of interactive electronic communication through
5 an internet website or application by which a user creates a service-specific
6 identifying user profile to connect with other users of the internet website or
7 application for the purpose of communicating and sharing information, ideas,
8 news, stories, opinions, images, videos, and other content.
9 b. "Social media platforms" are defined as the online digital services or websites that
10 facilitate social media.
11 c. "Message boards" are defined as digital services or websites that facilitate user
12 comments and/or replies about a particular issue or topic.
13 d. "Instant message services" are defined as online digital services or websites that
14 incorporate a function that permits real-time, text-based conversations between
15 users, whether or not such conversations are maintained or preserved.

16 Penalties for Improper Use of Network or Internet

17 Violation of this Policy or the Internet Safety and Acceptable Use Agreement referenced herein
18 may lead to disciplinary and/or legal consequences. Violations may result in student suspension
19 or expulsion, staff reprimand, suspension, or dismissal, or criminal prosecution by government
20 authorities for criminal offenses.

21 Privacy

22 No right to privacy exists in the use of BCS technology resources. Employees and students have
23 no expectation of privacy with regard to emails, internet activity, search histories, and/or
24 information and content housed on the hardware of any BCS owned technology. Users should
25 not assume that files or communications accessed, downloaded, created, or transmitted using
26 BCS technology resources or stored on services or hard drives of individual computers will be
27 private. BCS Technology staff, as directed by the Superintendent, may review files, monitor and
28 intercept messages, and otherwise monitor internet activity to maintain system integrity and to
29 ensure compliance with Board policies and applicable laws and regulations.

30 Internet Filtering

31 Bartlett City Schools will use technology protection measures on all district networks for all
32 Internet-enabled, district-owned devices to block or filter the access of material that violates this
33 BCS Acceptable Use Policy. The district reserves the right to monitor users' online activities and
34 to access, review, copy, and store or delete any electronic communication or files and disclose
35 them to third parties as it deems necessary and as is legally permissible. Users maintain no
36 expectation of privacy regarding their use of district owned or district provided technology,
37 including e-mail.

38 The categories of material considered inappropriate and to which access will be blocked will
39 include, but not be limited to: nudity/pornography; images or descriptions of sexual acts; profane
40 materials, obscene materials, materials promoting violence, illegal use of weapons, drug use,
41 discrimination, or participation in hate groups; instructions for performing criminal acts, and online
42 gambling.

43 The Superintendent or his/her designee will consider requests from users who wish to use a
44 blocked site for bona fide research or other lawful purposes. This permission will be granted for a

⁴ T.C.A. §49-6-4605

specific period of time and internet activity will be logged and reported to the district Network Administrator during this period.

Providers

Providers of digital or online resources with which BCS contracts for the provision of digital or online materials created and marketed for kindergarten (K) through grade twelve (12) shall:

1. Verify that the digital or online materials do not violate T.C.A. §39-17-902;
2. Take commercially reasonable steps to filter, block, or otherwise prevent access to pornography or obscenity through one's use of the digital or online materials;
3. Verify, in writing, that it has taken commercially reasonable steps to ensure that the provider's technology will prevent a user from sending, receiving, viewing, or downloading materials that are harmful to minors, as defined in T.C.A. §39-17-901; and
4. Remove, upon BCS's request, BCS's access to digital or online materials for ages or audiences for which BCS has determined the material to be age or audience-inappropriate. A provider must remove such BCS access within one (1) business day of the provider's receipt of BCS's request, unless the deadline for removal is extended by mutual consent of BCS and the provider.

If a BCS student, parent/guardian of a BCS student, or a BCS employee believes that a provider has not satisfied the aforementioned requirements, then a BCS student, the parent/guardian of a BCS student, or a BCS employee may file a complaint with the BCS Assistant Superintendent of Teaching and Learning or his/her designee specifically stating the alleged violation. The Assistant Superintendent of Teaching and Learning or his/her designee shall review each allegation of failure to fulfill the aforementioned requirements and shall advise the Complainant of whether he/she believes that action should be taken as it relates to the provider. This policy provision pertains to all contracts entered into with providers after July 1, 2022.

K-5 Technology Use

BCS remains committed to providing critical educational technology supports in an age-appropriate and instructional manner. The scope of this portion of the BCS Technology Use Policy is designed to minimize unnecessary screen time while preserving educational effectiveness and expanding teacher-led interactive instruction. This Policy applies to all K-5 student use of District-issued hardware, software applications, and network infrastructure during the instructional day.

Students in grades K-5 are strictly prohibited from accessing social media platforms through BCS-owned internet services or BCS-issued devices during the instructional day. Social media shall be blocked.

Each elementary school serving grades K-5 shall implement the following instructional guidelines:

1. Prioritization of Non-Electronic Instruction
 - a. In-person, teacher-led instruction and the use of physical, non-electronic materials will remain the primary mode of instruction for K-5 classrooms. BCS supports a blended approach to instruction where BCS-issued devices are not the sole physical instructional resources but serve as a tool for instruction. All students K-5 shall have access to physical copies of core textbooks.
2. Requirements for 1:1 Device Deployment
 - a. In the event K-5 students receive BCS-issued devices for the student's exclusive use, such devices will be used for tasks where there is a clear, demonstrable

educational benefit. Teachers must actively monitor screen interactions to ensure student engagement remains active rather than passive.

3. Passive Consumption Prohibited

a. Activities where students sit passively watching video content or interacting with software lacking explicit academic milestones are prohibited during the instructional day.

b. Only educational applications/programs approved by BCS Instructional Technology Department may be used by students in any BCS school.

c. Teachers must follow requirements for high quality instructional materials when utilizing digital platforms.

4. Active, Creative Use Encouraged

a. Activities are encouraged if they prioritize student agency, creative output, and adaptive, targeted skill practice. Such outputs include, but are not limited to, digital drawing, presentation building, coding concepts, etc.

All digital assessments, learning management platforms, and software applications used in grades K-5 shall be developmentally appropriate and directly mapped to the Tennessee Academic Standards. No software or online application shall be used unless approved by the BCS Department of Teaching and Learning.

At the start of each school year, each BCS elementary school shall publish a complete, accessible directory detailing the names and descriptions of all educational software and applications installed on K-5 student devices and the academic purpose of each tool and its direct connection to Tennessee state curriculum standards.

K-5 Technology Use policies and procedures do not prohibit the use of digital devices for:

1. Targeted instructional support, intervention, or remediation;
2. Accommodations or services required under the Individuals with Disabilities Education Act, Section 504 of the Rehabilitation Act, or the Americans with Disabilities Act;
3. Administration of a universal screener adopted by the State Board of Education, a Tennessee universal screener, dyslexia screenings, state-adopted benchmark assessments, or other assessments required by state or federal law;
4. Teacher preparation, lesson planning, or professional use;
5. Homebound instruction established in T.C.A. §49-10-1101;
6. Remote instructional days provided pursuant to T.C.A. §49-6-3004(i); or
7. Hybrid learning days provided pursuant to T.C.A. §49-6-3004).