The board provides its students and staff access to a variety of technological resources. These resources provide opportunities to enhance learning, appeal to different learning styles, improve communication within the school community and with the larger global community, and achieve the educational goals established by the board. Through the school system's technological resources, users can observe events as they occur around the world, interact with others on a variety of subjects, and acquire access to current and in-depth information.

The board intends that students and employees benefit from these resources while remaining within the bounds of safe, legal, and responsible use. Accordingly, the board establishes this policy to govern student and employee use of school system technological resources. This policy applies regardless of whether such use occurs on or off school system property, and it applies to all school system technological resources, including but not limited to computer networks and connections, the resources, tools and learning environments made available by or on the networks, and all devices that connect to those networks.

A. EXPECTATIONS FOR USE OF SCHOOL TECHNOLOGICAL RESOURCES

The use of school system technological resources, including access to the Internet, is expected to be exercised in an appropriate and responsible manner. Individual users of the school system's technological resources are responsible for their behavior and communications when using those resources. Responsible use of school system technological resources is use that is ethical, respectful, academically honest, and supportive of student learning. Each user has the responsibility to respect others in the school community and on the Internet. Users are expected to abide by the generally accepted rules of network etiquette.

General student and employee behavior standards, including those prescribed in applicable board policies, the Code of Student Conduct and other regulations and school rules, apply to use of the Internet and other school technological resources.

In addition, anyone who uses school system computers or electronic devices or who accesses the school network or the Internet using school system resources must comply with the additional rules for responsible use listed in Section B, below. These rules are intended to clarify expectations for conduct but should not be construed as all-inclusive.

Before using the Internet, all students must be trained about appropriate online behavior as provided in policy 3226/4205, Internet Safety.

All students and employees must be informed annually of the requirements of this policy and the methods by which they may obtain a copy of this policy. Before using school system technological resources, students and employees must agree to a statement indicating that they understand and will strictly comply with these requirements. Note: This is done each time staff and students log on by agreeing to current regulations. Failure to adhere to these

requirements will result in disciplinary action, including revocation of user privileges and fines due to the destruction of school property. Willful misuse may result in disciplinary action and/or criminal prosecution under applicable state and federal law, disciplinary action for students, and/or adverse personnel action for employees.

B. RULES FOR USE OF SCHOOL TECHNOLOGICAL RESOURCES

1. School system technological resources are provided for school-related purposes only. Acceptable uses of such technological resources are limited to responsible, efficient, and legal activities that support learning and teaching. Use of school system technological resources for commercial gain or profit is prohibited. Student personal use of school system technological resources for amusement or entertainment is also prohibited unless approved for special situations by the teacher or school administrator. Because some incidental and occasional personal use by employees is inevitable, the board permits infrequent and brief personal use by employees so long as it occurs on personal time, does not interfere with school system business, and is not otherwise prohibited by board policy or procedure.

2. Under no circumstance may software purchased by the school system be copied for personal use, unless specifically negotiated in the software company's user license agreement (ULA).

3. Students and employees must comply with all applicable laws, including those relating to copyrights and trademarks, confidential information, and public records. Any use that violates state or federal law is strictly prohibited. Plagiarism of Internet resources will be treated in the same manner as any other incidents of plagiarism, as stated in the Code of Student Conduct.

4. Users must follow any software, application, or subscription service terms and conditions of use.

5. No user of technological resources, including a person sending or receiving electronic communications, may engage in creating, intentionally viewing, accessing, downloading, storing, printing, or transmitting images, graphics (including still or moving pictures), sound files, text files, documents, messages, or other material that is obscene, defamatory, profane, pornographic, harassing, abusive or considered to be harmful to minors.

6. The use of anonymous proxies to circumvent content filtering is prohibited.

7. Users may not install or use any Internet-based file sharing program designed to facilitate sharing of copyrighted material.

8. Users of technological resources may not send electronic communications fraudulently (i.e., by misrepresenting the identity of the sender).

9. Users must respect the privacy of others. When using e-mail, chat rooms, blogs or other forms of electronic communication, students must not reveal personal identifying information, or information that is private or confidential, such as the home address or telephone number, credit or checking account information or social security number of themselves or fellow students. For further information regarding what constitutes personal identifying information, see policy 4705/7825, Confidentiality of Personal Identifying Information. In addition, school employees must not disclose on school system websites or web pages or elsewhere on the Internet any personally identifiable, private, or confidential information concerning students (including names, addresses or pictures) without the written permission of a parent or guardian or an eligible student, except as otherwise permitted by the Family Educational Rights and Privacy Act (FERPA) or policy 4700, Student Records. Users also may not forward or post personal communications without the author's prior consent. Students may not use school system technological resources to capture audio, video, or still pictures of other students and/or employees in which such individuals can be personally identified, nor share such media in any way, without consent of the students and/or employees and the principal or designee. An exception will be made for settings where students and staff cannot be identified beyond the context of a sports performance or other public event or when otherwise approved by the principal. School employees may disclose student information (such as name, photograph, or digital image) on school system websites and web pages unless parents/guardians/eligible students have opted out of the release of director information.

10. Users may not intentionally or negligently damage computers, computer systems, electronic devices, software, computer networks or data of any user connected to school system technological resources. Users may not knowingly or negligently transmit computer viruses or self-replicating messages or deliberately try to degrade or disrupt system performance, including by streaming audio or video for non-instructional purposed. Users may not disable antivirus programs installed on school system-owned or issued devices.

11. Users may not create or introduce games, network communications programs or any foreign program or software onto any school system computer, electronic device or network without the express permission of the technology director or designee unless gaming is an integral part of the curriculum.

12. Users are prohibited from engaging in unauthorized or unlawful activities, such as "hacking" or using the computer network to gain or attempt to gain unauthorized or unlawful access to other computers, computer systems or accounts.

13. Users are prohibited from using another individual's ID or password for any technological resource without permission from the individual. Sharing of an individual's ID or password is strongly discouraged. If an ID or password must be shared for a unique classroom situation, students must have permission from the teacher or other school official.

14. Users may not read, alter, change, block, execute or delete files or communications belonging to another user without the owner's express prior permission.

15. Employees shall not use passwords or user IDs for any data system (e.g., current student information system and instructional improvement system applications, CECAS, time-keeping software, etc.) for an unauthorized or improper purpose.

16. If a user identifies or encounters an instance of unauthorized access or another ~~a~~ security concern, on a technological resource, he or she must immediately notify a system administrator. Users must not demonstrate the problem to other users. Any user identified as a security risk will be denied access.

17. It is the user's responsibility to back up data and other important files.

18. Employees shall make reasonable efforts to supervise students' use of the Internet during instructional time.

19. Views may be expressed on the Internet or other technological resources as representing the view of the school system or part of the school system only with prior approval by the superintendent or designee.

20. Users who are issued school system-owned and -maintained devices for home use (such as laptops, Chromebooks, etc.) must adhere to any other reasonable rules or guidelines issued by the superintendent or technology director for the use of such devices.

C. RESTRICTED MATERIAL ON THE INTERNET

The Internet and electronic communications offer fluid environments in which students may access or be exposed to materials and information from diverse and rapidly changing sources, including some that may be harmful to students. The board recognizes that it is impossible to predict with certainty what information on the Internet students may access or obtain. Nevertheless, school system personnel shall take reasonable precautions to prevent students from accessing material and information that is obscene, pornographic, or otherwise harmful to minors, including violence, nudity, or graphic language that does not serve a legitimate pedagogical purpose. The superintendent shall ensure that technology protection measures are used as provided in policy 3226/4205, Internet Safety, and are disabled or minimized only when permitted by law and board policy. The board is not responsible for the content accessed by using a cellular network to connect a personal device to the internet.

D. PRIVACY

No right of privacy exists in the use of technological resources. Users should not assume that files or communications created or transmitted using school system technological resources or stored on services or hard drives of individual computers will be private. School system administrators or individuals designated by the superintendent may review files, monitor all communication, and intercept e-mail messages to maintain system integrity and to ensure compliance with board policy and applicable laws and regulations. School system personnel shall monitor online activities of individuals who access the Internet via a school-owned computer.

E. PERSONAL WEBSITES

The superintendent may use any means available to request the removal of personal websites that substantially disrupt the school environment or that utilize school system or individual school names, logos, or trademarks without permission.

1. Students

   Though school personnel generally do not monitor students' Internet activity conducted on non-school system devices during non-school hours, when the student's online behavior has a direct and immediate effect on school safety or maintaining order and discipline in the schools, the student may be disciplined in accordance with board policy (see the student behavior policies in the 4300 series).

2. Employees

   Employees' personal websites are subject to policy 7335, Employee Use of Social Media.

3. Volunteers

   Volunteers are to maintain an appropriate relationship with students at all times. Volunteers are encouraged to block students from viewing personal information on volunteer personal websites or online networking profiles in order to prevent the possibility that students could view materials that are not age appropriate. An individual volunteer's relationship with the school system may be terminated if the volunteer engages in inappropriate online interaction with students.

F. LIABILITY LIMITATIONS AND DISCLOSURES

While BCS will always strive to provide the most efficient, safe, and appropriate resources reliably, the technological complexity of this mission makes guarantees impossible. By agreeing to Board Policy 3220, users recognize that BCS will not be held responsible in the

event that service does not meet user expectations. Users also express their awareness that any information created or stored within the BCS network is not private by agreeing to board policy.

a. BCS makes no warranties of any kind, whether expressed or implied, for the services provided. BCS is not responsible for damages suffered, including the loss of data resulting from delays, non-deliveries, or service interruptions caused by its own negligence or the user's errors or omissions, or loss/damage to personal devices. Use of any information obtained via the Internet is at user's own risk. BCS specifically denies any responsibility for the accuracy or quality of information obtained through its services.

b. The inclusion of any link to a site not controlled by BCS is for convenience only and does not represent an endorsement of the site by BCS. Students, parents, and staff should be aware that connection to any Internet or network provider not under BCS control may be unfiltered. This is particularly true of open wireless connections which are widely available and through Internet enabled smart telephone access. BCS is not responsible for unfiltered content that may be viewed or downloaded on BCS equipment that has been provided to individuals for use outside BCS network control or property. BCS will, however, remove said inappropriate content from equipment owned by BCS and will ask that, in the case of proven inappropriate content, equipment not owned by BCS be removed from school property.

c. The board recognizes that parents of minors are responsible for setting and conveying the standards their children should follow when using media and information sources. Accordingly, before a student may independently access the Internet, the student's parent must be made aware of the possibility that the student could obtain access to inappropriate material while engaged in independent use of the Internet. The parent and student must consent to the student's independent access to the Internet and to monitoring of the student's e-mail communication by school personnel. In addition, in accordance with the board's goals and visions for technology, students may require accounts in third party systems for school related projects designed to assist students in mastering effective and proper online communications or to meet other educational goals. Parental permission will be obtained when necessary to create and manage such third- party accounts. Students & staff are prompted to agree to current policies during each device log in.

G. USE AGREEMENTS

All students, parents, and employees will be informed annually of the information in this policy and in any applicable generative artificial intelligence (AI) guidelines developed in accordance with policy 3220, Technology in the Educational Program. Prior to using school system technological resources, students and employees must agree to comply with the requirements of this policy and the generative AI guidelines and consent to the school system's use of monitoring systems to monitor and detect inappropriate use of technological

resources. In addition, the student's parent must consent to the student accessing the Internet and to the school system monitoring the student's Internet activity and electronic mailbox issued by the school system and must sign a copy of the generative AI guidelines.

Annual Public Notices are posted online at www.buncombeschools.org and are also included in the student handbook for information. A hard copy of this notice will be provided upon request.

Legal References: U.S. Const. amend. I; Children's Internet Protection Act, 47 U.S.C. 254(h)(5); Electronic Communications Privacy Act, 18 U.S.C. 2510-2522; Family Educational Rights and Privacy Act, 20 U.S.C. 1232g; 17 U.S.C. 101 *et seq.*; 20 U.S.C. 7131; G.S. 115C-325(e) (applicable to career status teachers), -325.4 (applicable to non-career status teachers)

Cross References: Curriculum and Instructional Guides (policy 3115), Technology in the Educational Program (policy 3220), Internet Safety (policy 3226/4205), Copyright Compliance (policy 3230/7330), Web Page Development (policy 3227/7322), Student Behavior Policies (all policies in the 4300 series), Student Records (policy 4700), Confidentiality of Personal Identifying Information (policy 4705/7825), Public Records – Retention, Release and Disposition (policy 5070/7350), Use of Equipment, Materials and Supplies (policy 6520), Network Security (policy 6524), Staff Responsibilities (policy 7300), Employee Use of Social Media (policy 7335)

Other Resources: North Carolina Generative AI Implementation Recommendations and Considerations for PK-13 Public Schools, available at https://go.ncdpi.gov/AI_Guidelines

Replaced Board Policy 646

History of Policy 646
Adopted: May 3, 2012
Revised: October 5, 2023
Revised: June 5, 2025

NCSBA wording and revision to Policy 646 adopted: December 12, 2013
NCSBA Update: Fall 2016 (Did not affect content)

BUNCOMBE COUNTY SCHOOLS
EMPLOYEE CONFIDENTIALITY STATEMENT

Introduction: A moral and legal obligation is placed upon computer technicians, data managers, teachers, and supervisors to treat information accessible through data base retrieval by electronic or paper as confidential information. The law and the courts have recognized a person's right to have personal information treated confidentially. Buncombe County School personnel or others allowed with working access to such information must be trusted to protect sensitive information from becoming public knowledge.

Therefore: Personnel or representatives of Buncombe County Schools agree to hold confidential any and all information gained by access to another student's, parent's, or employee's (here-by referred to as client) data records. These include, but are not exclusive to, system access passwords, personal medical status, grades, test scores, personnel action, or impending personnel status. Personnel or representatives with such access will protect the information from becoming public knowledge. They will not discuss any client information with others either in private or public (unless by law, regulation, contract, or policy that client information is required to be shared with another co-lateral responsible person or organization with the need to know).

The client is assured of confidential treatment of records and disclosures and is afforded the opportunity to approve or refuse the release of that data to any individual except as required by law. Each person or representative that has electronic database or paper access to privileged information, as required by his supervisor, shall sign this confidentiality statement. The confidentiality statement is forever: the agent is bound not to discuss any client information gained while employed in Buncombe County Schools, even after they terminate employment, or agent position. A signed copy of the Assurance of Confidentiality form will be placed in an appropriate personnel file.

EMPLOYEE ASSURANCE OF CONFIDENTIALITY
I understand and agree to comply with the Confidentiality Statement of Buncombe County Schools, the purpose of which is to insure the privileged and confidential nature of client information. I have read and acknowledge Board of Education Policy 3220 and Board of Education Administrative Regulation regarding Policy 3220. In accordance with this statement, I agree to hold CONFIDENTIAL all information about clients or former clients served by Buncombe County Schools to which I may have access and agree to not divulge such confidential information to unauthorized persons or third- party entities.

I understand that all information, not otherwise protected from disclosure by law, may be disclosed to third parties at the discretion of the Superintendent of the BCS or an appointed designee.
I also understand that my failure to comply with this statement may result in suspension or dismissal from employment and/or legal action. A copy of this agreement shall be maintained in the employee's personnel file.

Signed _____ Date _____