Policy Code: 3225/4312/7320 Technology Responsible Use

The Board provides its students and staff access to a variety of technological resources. Technological resources, including computers, other electronic devices, programs, networks and the Internet, 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 effective and responsible use of technology, the district can advance learning for every student and produce competent users who are workforce-ready citizens.

North Carolina Department of Instruction requires the use of technology in schools for a number of different purposes, including online State assessments, the integration and implementation of the Digital Learning Standards for Students, the Digital Learning Competencies for Teachers, Instructional Support Staff and Administrators, and the North Carolina Professional Teaching Standards.

The Board intends that students and employees benefit from these technological resources while remaining within the bounds of safe, legal, responsible, and effective 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, digital tools and resources, and learning environments made available by or on the networks, and all devices that connect to those networks.

Technological resources should be aligned to current state and national standards and integrated into the educational program in order to enhance and deepen student learning. The use of technology should be evaluated in an ongoing manner, with feedback solicited from all stakeholders regarding successes, challenges, and possible areas for improvement.

Professional personnel will make thoughtful use of technological resources by considering the following criteria[1]:

- **Whether use is purposefully integrated to support and deepen student learning.** Technology, like all educational resources, should be used thoughtfully and intentionally for specific outcomes. Technology should be considered along with additional offline learning activities to achieve a healthy balance.
- **Whether use is solitary or collaborative.** Collaborative and interactive use of technology appears to have a positive impact on social skills, whereas passive, solitary use may be harmful to social development.
- **Whether use is sedentary or mobile**. Sedentary use of any resource for extended periods of time, including technology, is discouraged as sedentary action has been linked to obesity and other undesirable outcomes. Noting the importance of play in early childhood development, using active, experiential learning to support the use of technology is essential. Furthermore, recess in kindergarten through fifth grade should be device-free whenever possible and encourage unstructured playtime.
- **Content and features of the technological resources are evaluated.** Content should be regularly evaluated to ensure it is appropriate and engaging for the intended children and desired learning outcomes, avoiding violence and bias in language and characters.
- **Total screen time.** Screen time should be considered in combination with the other learning activities and resources students are using, rather than limited to an arbitrary time allotment, such as one hour a day. Screen time should be interactive and promote positive and

developmentally appropriate learning.

Teachers and other staff members will help students develop skills to enable them to effectively utilize devices and networks, and to search the Internet responsibly.

Professional personnel should consult Board Policy 3200, Selection of Textbooks and Supplementary Materials, for guidance on criteria for selecting digital instructional materials. The curriculum committee should provide suggestions for using technology resources in the curriculum guides as provided in Board Policy 3115, Curriculum and Instruction Guides. Teachers are encouraged to further incorporate the use of technological resources into their lesson plans when these resources are aligned with the lesson objective and directly support and enhance student learning.

The superintendent or designee shall ensure that school district devices with Internet access comply with federal requirements regarding filtering software and Internet safety policies. The superintendent or designee shall develop any regulations necessary to meet such requirements and will submit any certifications necessary to meet such requirements.

A. Expectations for Use of School Technological Resources

1. Any users of district technological resources, including staff and students, must comply with the requirements for use established in the administrative regulation which further defines or explains acceptable use, responsibilities of the user, limits of use, restricted material, consequences of unacceptable behavior, confidentiality of information, and the inability of the Board to guarantee services on the Internet.

2. 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 lawful, 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 digital citizenship.

3. General student and employee behavior standards, including those prescribed in applicable Board policies, the Code of Student Conduct, Character, and Support and other regulations and school rules, also apply to use of school technological resources, including access to the Internet. All students must be trained about appropriate online behavior. Such training must cover topics such as cyberbullying awareness and response, and interacting with others on social networking websites and in chat rooms.

4. 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.

5. Failure to adhere to the requirements of this policy will result in disciplinary action, including revocation of user privileges. Willful misuse may result in disciplinary action for students and/or adverse personnel action for employees and/or criminal prosecution under applicable state and federal law, disciplinary action for students 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. Personal use of school system technological resources for amusement or entertainment is prohibited unless approved for special situations by the teacher, school leader, or district 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. Unless authorized by law to do so, users may not make copies of software purchased by the school system. Under no circumstance may software purchased by the school system be copied for personal use.

3. Users must comply with all applicable laws, board policies, administrative regulations, and school standards and rules, including those relating to copyrights and trademarks, confidential information, and public records. 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, Character, and Support.

4. Users must follow any software, application, or subscription services 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 virtual private network or proxy software to bypass network security and content filtering systems and circumventing firewalls 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.

a. Students must not reveal any personally identifying, private, or confidential information about themselves or fellow students when using e-mail, chat/messaging, blogs, videoconferencing, or other forms of electronic communication. Such information includes, for example, a person’s home address, or telephone number, credit or checking account information, or social security number. For further information regarding what constitutes personal identifying information, see policy 4705/7825, Confidentiality of Personal Identifying Information.

b. 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 a guardian, or an eligible student, except as otherwise permitted by the Family Educational Rights and Privacy Act (FERPA) or policy 4700, Student Records.

c. Users may not forward or post personal communications without the author's prior consent.

d. 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.

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 purposes. 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 non-approved program or software, including remote access (virtual private network, web proxy) onto any school system computer, electronic device or network without the express permission of the Executive Director of Technology or designee.

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, electronic devices, computer systems, or accounts.

13. Users are prohibited from sharing assigned IDs and passwords.

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., the state student information and instructional improvement system applications, time-keeping software, etc.) for an unauthorized or improper purpose.

16. If a user identifies or encounters an instance of unauthorized access or another security concern, he or she must immediately notify a teacher, school system administrator, or the Executive Director of Technology or designee. Users must not share the problem with 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 monitor students' use of the Internet on district-provided devices 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 and/or the Executive Director of Technology for the use of such devices.

C. Restricted Material on the Internet

All users are responsible for their actions when using technological resources. Access to networks is available to individuals willing to act responsibly and courteously. Use of networked resources in a manner harmful to others will not be tolerated. Use of district technological resources will comply with administrative regulations developed by the superintendent.

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 (such as Internet filtering) 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.

Since no content filtering solution provides 100% protection from inappropriate materials, such as violence, nudity, obscenity, or graphic language that does not serve a legitimate pedagogical purpose, the user is ultimately responsible for his or her activity on the Internet. School officials may disable such filters for an adult who uses a school owned computing device for bona fide research or other lawful educational purposes. School system personnel may not restrict Internet access to ideas, perspectives, or viewpoints if the restriction is motivated solely by disapproval of the ideas involved.

D. Essential Technology:

District-provided technology resources including use of district-provided student devices, digital textbooks and subscriptions, online testing, virtual courses, remote learning, and learning management systems are essential teaching tools. While an opt-out from essential technologies is not available, parents/guardians are encouraged to discuss any concerns regarding technology with their child’s teacher and school administrators. The Board requires district staff with the assistance of school staff, to ensure any contract and/or agreement with a third-party service that receives student information, uses the data only for authorized purposes and protects the data from future disclosures.

In accordance with the Board's goals and visions for technology, students may require accounts in third party systems to be used independently for school related projects designed to assist students in mastering effective and proper online communications or to meet other educational goals. The Children's Online Privacy Protection Act (COPPA) allows schools to act as agents for parents in providing consent for the creation of student accounts within the school context if the information collected is used for internal operations only and is not shared with outside organizations.

E. Privacy

The Chapel Hill-Carrboro City Schools shall take reasonable measures to protect the privacy of its technology resources and accounts assigned to authorized users. However, the Chapel Hill-

Carrboro City Schools cannot guarantee absolute security and privacy. In addition, any activity on Chapel Hill-Carrboro City Schools technology resources may be monitored, logged and reviewed by Chapel Hill-Carrboro City Schools approved personnel or may be discovered in legal proceedings or in response to public records requests. Circumstances that may result in the examination of user accounts include, but are not limited to, the following:

- when required for system maintenance or business necessity, including security measures;
- when there exists reason to believe an individual is violating the law or any applicable policies or regulations;
- when needed to investigate reports of misconduct towards students, staff, or others;
- to meet the requirements of the North Carolina Public Records Law or other laws, regulations, or institutional policies, rules, or guidelines, or
- as permitted by applicable law or policy.

The Chapel Hill-Carrboro City Schools have the right to employ appropriate security measures, to investigate as needed, and to take necessary actions to protect students, staff, and Chapel Hill-Carrboro City Schools technology resources.

Under certain circumstances, school officials may be required to disclose such electronic information to law enforcement or other third parties, for example, as a response to a document production request in a lawsuit against the board, in response to a public records request, or as evidence of illegal activity in a criminal investigation. Chapel Hill-Carrboro City Schools will work with authorized users to protect student and staff privacy interests, as well as those of the Chapel Hill-Carrboro City Schools.

Authorized users must not violate the privacy of other users. Technical ability to access unauthorized resources or others’ accounts does not by itself imply authorization to do so, and it is a violation of this policy to access others’ accounts unless authorized to do so for a legitimate business purpose.

Students, employees, visitors, and other users should have no right of privacy in anything they create, store, send, delete, receive, or display when using the school system's networks including WiFi access on a district or personal device, internet access, email system, or other technological resources owned or issued by the school system, whether the resources are used at school or elsewhere, and even if the use is for personal purposes.

When student information may be transmitted to a vendor of school technology resources, district staff shall ensure that the resource is acquired through a written contract that ensures the vendor and any other party who receives student information will use the data only for authorized purposes and will protect the data from future disclosures to at least the standard required under the Family Educational Rights and Privacy Act.

School network spaces are analogous to desks or lockers and may be inspected when network maintenance becomes necessary if users are suspected of abusing access rights, and/or to ensure compliance with board policy and applicable laws and regulations.

Users should not assume that files or communications created, transmitted, or displayed using district-managed technological resources or stored on servers or on the storage mediums of individual devices, or on school managed cloud services will be private. The school system may, without notice, (1) monitor, track, and/or log network access, communications, and use; (2) monitor physical and virtual data storage; and (3) access, review, copy, store, delete, or disclose the content of all user files, regardless of medium, the content of electronic mailboxes issued by the school system, and system outputs, such as printouts, at any time for any lawful purpose. Such purposes may include, but are not limited to maintaining system integrity, security, or functionality, ensuring compliance with board policy and applicable laws and regulations, protecting the school system from liability, and complying with public records requests.

School system personnel shall monitor online activities of individuals who access the Internet via the district network, a school owned device, or school managed cloud services via personal computers, or devices. By using the school system's network, Internet access, email system, electronic devices, or other technological resources, individuals consent to have that use monitored by authorized school system personnel as described in this policy.

F. Use of Personal Technology on School System Property

Users may not use private WiFi hotspots or other personal technology on campus to access the Internet outside the school system’s wireless network. Each principal may establish rules for his or her school site as to whether and how other personal technology devices (including, but not limited to smart phones, tablets, laptops, etc.) may be used on campus. Students’ devices are governed also by policy 4318, Use of Wireless Communication Devices. Use of personal technology devices is also subject to any rules established by the superintendent under a bring your own device plan authorized by Section C of policy 3220, Technology in the Educational Program. The school system assumes no responsibility for personal technology devices brought to school.

G. Personal Websites

The superintendent may use any means available to request the removal of personal websites, social networking websites, and other forms of online materials and communications that substantially disrupt the school environment or that utilize names, logos, or trademarks of the school district or individual schools without permission.

1. Students

School personnel generally do not monitor students' Internet activity conducted on non-I school system devices during non-school hours. School personnel do have the capability to monitor activity in cloud-based systems managed by the district. When the student's online behavior, using the Internet or district managed services, 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 to the extent consistent with law (see student behavior policies in the 4300 series).

2. Employees

In accordance with Policy Code 7300 Staff Responsibilities and Ethics, the board expects all staff members to conduct themselves on and off the job in a manner that not only reflects positively on the school system, but that sets forth a model worthy of emulation by students. This expectation includes the use of personal websites, social networking websites, and other forms of online materials and communications. Employees’ personal websites are subject to policy 7335, Employee Use of Social Media. Employees may not use their personal websites to communicate with students, as prohibited by policy 7335 and policy 4040/7310, Staff-Student Relations.

All employees must use district provided tools when communicating with students about any school related matters except as permitted in Policy 4040/7310 Staff-Student

Relations.

Employees are to maintain appropriate relationships with students at all times.

Employees are encouraged to block students from viewing personal information on employee personal websites or social networking profiles in order to prevent the possibility that students could view materials that are not age appropriate. If an employee creates and/or posts inappropriate content on a website or profile and it has a negative impact on the employee's ability to perform his or her job as it relates to working with students, the employee will be subject to discipline up to and including dismissal. This section applies to all employees, volunteers, and student teachers working in the school system.

3. Volunteers

Volunteers are to maintain appropriate relationships 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.

H. Accessibility

All district technology, including resources considered to be essential to the district mission, must be selected, used, and supplemented or modified in a manner that provides equal access and/or an equivalent opportunity for students with disabilities, second language students, and other special needs.

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), -325.4, 391, Children's Online Privacy Protection Act, 59888 Federal Register/Vol. 64, No. 212 / 3972 Federal Register/ Vol. 78, No.12.

Cross References: Curriculum and Instructional Guides (policy 3115), Technology in the Educational Program (policy 3220), Copyright Compliance (policy 3230/7330), Web Page Development (policy 3227/7322), 4040/7310 Staff-Student Relations, Student Behavior Policies (all policies in the 4300 series), Student Records (policy 4700), Use of Equipment, Materials and Supplies (policy 6520), Staff Responsibilities (policy 7300), Employee Use of Social Media (policy 7335).

References: [1] “Healthy & Effective Technology Use: Moving from Screen Time to Effective Practice,” March 2019, Prepared by John D. Ross, Ph.D. for Arlington Public Schools, VA and Baltimore County School Health Council Workgroup Report: “Health Guidance for the Digital Classroom,” June 2018

Adopted: 11/20/97

Revised: 3/23/00, 2/7/02, 7/20/06, 2/3/11, 8/15/2013, 5/21/15, 10/5/16, 4/12/23