

Policy Code: 3225/4312/7320 Technology Responsible Use

The Currituck County Board of Education provides its students and staff access to a variety of technological resources. These resources provide opportunities to enhance learning and improve communication within the school community and with the larger global community. 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 a privilege, not a right. 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. All students and employees must receive a copy of this policy annually. At the beginning of each school year, students and employees must sign a statement indicating that they understand and will strictly comply with these requirements and acknowledging awareness that the school system uses monitoring systems to monitor and detect inappropriate use of technological resources. Failure to adhere to these requirements will result in disciplinary action, including possible revocation of user privileges. Willful misuses may result in disciplinary action and/or criminal prosecution under applicable state and federal law.

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 political or commercial gain or profit is prohibited. Student personal use of school system technological resources for amusement or entertainment is also prohibited during instructional hours. 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 the appropriate licenses have been secured.
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. 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. All users must comply with policy 1710/4021/7230, Prohibition Against Discrimination, Harassment and Bullying, in using technological resources.
5. The use of anonymous proxies to circumvent content filtering is prohibited.
6. Users may not install or use any Internet-based file sharing program designed to facilitate sharing of copyrighted material.
7. Users of technological resources must not post information that could be disruptive, cause damage or endanger students or staff.
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, except for designated directory information set forth in policy 4700, Student Records, and as permitted by the Family Educational Rights and Privacy Act (FERPA), without the written permission of a parent or guardian or an eligible student. Directory information will not be posted if a parent or eligible student has opted out of having this information disclosed. When student pictures or student work is posted only the student's first name shall be used. Users also may not forward or post personal communications without the author's prior consent.

10. Users are required to follow any board policies or procedures regarding maintenance or care of equipment. 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.

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. If such permission is obtained, the use of the software will also be subject to any restrictions imposed by the technology director 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, computer systems or accounts. Users are prohibited from attempting to circumvent the Internet filtering system.

13. Users are prohibited from using another individual's ID or password for any technological resource without permission from the individual. Students must also 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., the state student information and instructional improvement system applications, time-keeping software, etc.) for an unauthorized or improper purpose.

16. If a user identifies a security problem 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. Teachers and administrators shall make reasonable efforts to supervise a student's use of the Internet during instructional time in a manner appropriate to the student's age and the circumstances of use.

18. 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.

19. Users may use personal computing devices (smartphones, tablets, laptops, etc.) on the school network with supervisor's or principal's permission. The school district is not responsible for damage, loss, or theft of personal computing devices. Users are subject to all aspects of this policy when using personal computing devices in the schools and on the school network. The technology department will not provide support for personal computing 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 materials 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 users who connect to the Internet via their personal mobile telephone technology (e.g., 3G, 4G service).

D. Parental Consent

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 provide written consent to the student's independent access to the Internet and to monitoring of the student's Internet activity and 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 not controlled by the school district 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.

E. Privacy

Students, employees, visitors, and other users have no expectation of privacy in anything they create, store, send, delete, receive, or display when using the school system's network, devices, 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. Users should not assume that files or communications created, transmitted, or displayed using school system technological resources or stored on servers or on the storage mediums of individual devices will be private. The school system may, without notice, (1) monitor, track, and/or log network access, communications, and use; (2) monitor and allocate files server space; and (3) access, review, copy, store, delete, or disclose the content of all user files, regardless of medium, the content of electronic mailboxes, and system outputs, such as printouts, 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 on-line activities of individuals who access the Internet via a school-owned device.

By using the school system's network, Internet access, email system, 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

Each principal may establish rules for his or her school site as to whether and how 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. 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 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 on-line 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

All employees must use school system controlled resources, or other systems approved by the employee's supervisor, as the primary means of communicating with students about any school-related matters.

Employees are to maintain an appropriate relationship with students at all times. Employees are encouraged to block students from viewing personal information on employee personal websites or on-line 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.

Employees shall not knowingly allow students access to their personal social networking sites that discuss or portray sex, nudity, alcohol or drug use or other behaviors associated with the employees' private lives that would be inappropriate to discuss with a student at school.

Employees shall be professional in all internet postings related to or referencing the school system, students and other employees.

Employees shall not use internet postings to libel or defame the board, individual board members, students or other school employees.

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 on-line 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. Waiver of Responsibility

The board makes no warranties of any kind, whether express or implied, for the technological services it provides. The board will not be responsible for any damage suffered by users, including loss of data resulting from delays, non-delivery, service interruptions or any other cause. Use of any information obtained from the Internet is at the user's risk. The board denies any responsibility for the accuracy or quality of information obtained through its Internet service. Users may be held responsible for any losses sustained by the board from a user's intentional misuse of the system's technological resources.

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), [-390.2](#)

Cross References: Prohibition Against Discrimination, Harassment and Bullying (policy 1710/4021/7230), Curriculum and Instructional Guides (policy 3115), Technology in the Educational Program (policy 3220), Internet Safety (policy 3226/4205), Web Page Development (policy 3227/7322), Use of Personal Technology to Conduct School Business (policy 3228/7323), Copyright Compliance (policy 3230/7330), 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)

Adopted: March 12, 2012

Revised: June 28, 2013; August 7, 2014, November 6, 2014; June 30, 2016, November 3, 2016; February 2, 2017; December 19, 2019 (cross reference only)

Currituck County Schools New Policy Manual
