

Policy Code: 7720 Employee Community and Political Activities

A. Community Activities

The board encourages participation in community activities by school personnel, not only to fulfill general citizenship responsibilities, but also as an effective method for increasing general public awareness of the school district and for promoting a progressive community spirit among its patrons. The board shall not limit or discourage participation in community activities, including public appearances, unless such participation could cause or causes significant interference with the activities of the school district or with the individual employee's ability to function effectively in the school community.

In their relationships with community groups, staff members should make a conscientious effort to make school life a part of community life and to bring the community close to the schools. Staff members should endeavor to know the community and its influences on, and opportunities for, students.

Staff members are reminded that the community may view them as representatives of the school district. However, staff members shall not claim or hold themselves out to be official school district representatives unless they have been so designated by the superintendent or the board.

B. Political Activities

The employee's right of citizenship involving registering, discussing political issues, voting, campaigning for candidates or issues, running for or serving in public office, and participating on a committee or board which seeks to serve the welfare of the community, will not be infringed upon due to employment in the school district.

These political activities will not:

1. take place during school time;
2. involve school monies or materials;
3. make use of an official school position to encourage or to coerce students or other employees of the district to support in any way a political party, candidate or issue; or
4. be presented as the views of the school district or of the employee in his/her official capacity as an employee of the school district.

Employees shall use good judgment and discretion when discussing political issues with students. Employees shall not promote personal political agendas while performing job duties.

As specified in Policy 2220, Official School Spokesperson, the board chair of the board or designee and the superintendent or designee are the official spokespersons for the school system. Employees, when exercising their rights as citizens, should take steps to ensure that their personal political opinions are not erroneously attributed to the school board or the school system.

This policy should not be construed as prohibiting the impartial study and discussion of political or other controversial issues in the classroom setting.

Legal References: [G.S. 115C-47\(18\)](#)

Cross References: Official School Spokesperson (Policy 2220)

Adopted: May 1, 1978

Revised: November 18, 2004, May 9, 2017; June 14, 2021

Cabarrus County Schools

Policy Code: 3225/4312/7320 Technology Responsible Use

Technological resources, including computers, smartphones, tablets, e-readers, other electronic devices, programs, networks and the Internet, provide opportunities to enhance instruction, appeal to different learning styles and meet the educational goals of 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.

Use of technological resources should be integrated into the educational program. For this policy, the term "Technological resources" will refer to resources that are owned, leased, maintained, or otherwise controlled by the school system. Technological resources should be used in teaching the North Carolina Standard Course of Study and in meeting the educational goals of the board. The curriculum committee should provide suggestions for using technological resources in the curriculum guides/frameworks as provided in Policy 3115, Curriculum and Instructional Guides/Frameworks for Instruction. Teachers are encouraged to further incorporate the use of technological resources into their lesson plans.

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

A. Requirements for Use of Technological Resources

The use of school system technological resources, such as computers, smartphones, tablets, e-readers and other electronic devices, networks, and the Internet, is a privilege, not a right for employees and students.

Annually, all students and staff must be trained about appropriate on-line behavior. Such training must cover topics such as cyberbullying and interacting with others on social networking websites and in chat rooms.

Anyone who uses school system computers, electronic devices, or personal devices at a Cabarrus County Schools location, or who accesses the school network or the Internet at an educational site, must comply with the requirements listed below. All students and employees must receive notice of this policy's provisions annually. Before using school system technological resources, students and employees must sign a statement indicating that they understand and will strictly comply with these requirements and acknowledge 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 revocation

of user privileges. Willful misuses may result in 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 activities that support learning and teaching. Use of school system technological resources for commercial gain or profit is prohibited. The superintendent or designee will provide guidelines to ensure that any Wi-Fi hotspots used off school system property were not purchased using E-Rate funds.
2. Under no circumstance may software purchased by the school system be copied for personal use.
3. Students and employees must comply with all applicable board policies, administrative regulations, and school standards and rules in using technological resources. All applicable laws, including those relating to copyrights and trademarks, confidential information, and public records, apply to technological resource use. 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 *Student Code of Conduct*.
4. No user of technological resources, including a person sending or receiving electronic communications, may engage in creating, intentionally 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 or considered to be harmful to minors.
5. Users must not circumvent firewalls. 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 may not send electronic communications fraudulently (i.e., by misrepresenting the identity of the sender).
8. 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 email, chat rooms, blogs, artificial intelligence (AI) tools 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, including generative AI tools or services, 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.
 - c. Students and employees shall not input, upload, or otherwise disclose personally identifiable information (PII) or confidential data into unapproved AI tools, including but not limited to free, public, or consumer-grade generative AI platforms. Such actions may constitute unauthorized data sharing under FERPA, the North Carolina Student Data Privacy Act, or other applicable laws.
 - d. Users may not forward or post personal communications without the author's prior consent.
 - e. 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 recordings or pictures in any way, without the consent of the other students and/or employees and the principal or designee. An exception will be made for recordings at events that are open to the public, such as athletic competitions, band and choral concerts, assemblies, presentations, and award ceremonies. If recording at a public event is restricted for any reason, including due to copyright issues (e.g., a school play), students, employees, and all other members of the audience will be notified of the recording restrictions before the event begins.
 - f. AI-Generated Images and Synthetic Media. Students and employees shall not use AI or other digital tools to create, distribute, or possess any image, video, or audio content that is sexually explicit (including synthetic or 'deepfake' depictions), depicts bullying, harassment, or humiliation of any person, or that defames, intimidates, or threatens others. This prohibition includes non-consensual intimate images (NCII) and any AI-generated or manipulated media reasonably likely to cause harm, embarrassment, or disruption to the school environment. Violations of this subsection are subject to disciplinary action consistent with this policy and applicable law.
9. Users may not intentionally or negligently damage computers, computer systems, electronic devices, software, or computer networks. Users may not

- knowingly or negligently transmit computer viruses or self-replicating messages or deliberately try to degrade or disrupt system performance.
10. Users may not create, download, or access any software (including, but not limited to, instructional, games, or network communications programs) onto any school system computer, electronic device or network without the express permission of the Chief Information Officer or designee.
 11. 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, accounts, data, or information.
 12. Users are prohibited from using another individual's computer account. Users may not read, alter, change, execute or delete files belonging to another user without the owner's express prior permission.
 13. Users may not read, alter, change, block, execute, or delete files or communications belonging to another user without the owner's express prior permission.
 14. Employees shall not use passwords or user IDs for any data system, state student information and instructional improvement system applications time-keeping software, etc. for an unauthorized or improper purpose.
 15. If a user identifies a security problem on a technological resource, he or she must immediately notify a system administrator. Users must not share the problem with other users. Any user identified as a security risk will be denied access.
 16. Cabarrus County School employees shall supervise student use of the Internet during instructional time.
 17. Cabarrus County School employees shall not use school system technological resources to promote personal, political, or religious viewpoints.
 18. Views may be expressed as representing the official view of the school system only with prior approval by the superintendent or designee.
 19. Students are prohibited from using their personal devices as private Wi- Fi hotspots during instructional hours.

Exceptions to these rules may be made for employees whose activities are necessary to carry out their job responsibilities and are authorized by law.

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 age-inappropriate, or harmful to minors, including violence, nudity, or graphic language that does not serve a legitimate pedagogical purpose as well as websites, web applications, or software that do not protect against the disclosure, use, or dissemination of a student's personal information. The superintendent or designee shall ensure 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 parents of minors are responsible for setting and conveying the standards their children should follow when using media and information sources. Before a student may use the Internet for any purpose, the student's parent must be made aware of the possibility that the student could obtain access to inappropriate material. Student users are responsible for appropriate use of the Internet and consent to monitoring by school system personnel of the student's e-mail communication and use of the Internet (Policy 4313 Student Use of Social Networking Sites, Blogging and the Internet). A student's use of a personal device to access the Internet at school subjects the student's internet activity and email communications to monitoring by school personnel as stated in Policy 4318, Use of Electronic Devices, and Policy 4342 Student Searches.

The board is aware there is information on the Internet that is not related to the educational program. The board is also aware the Internet may provide information and opportunities to communicate on subjects that are not suitable for school-age children and that many parents would find objectionable. School system personnel shall take reasonable precautions to prevent students from having access to inappropriate materials, such as violence, nudity, obscenity or graphic language that does not serve a legitimate pedagogical purpose. The superintendent or designee shall ensure the Internet service provider or technology personnel have installed a technology protection measure which blocks or filters Internet access to audio or visual depictions that are obscene, are considered pornographic or are harmful to minors. School officials may disable such filters for an adult who uses a school-owned computer for bona fide research or another lawful educational purpose. 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.

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

1. Students

Though school personnel generally do not monitor students' Internet activity conducted on non-school system computers 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 the school system e-mail or school system websites or webpages when communicating in their official capacity with students or parents on-line about any school-related matters. Thus, employees may not use personal websites, personal email accounts, or personal social media to communicate in their official capacity regarding school-related matters or attempt to communicate with other employees or students about school-related matters.

This prohibition is not intended and shall not be applied so as to prevent employees from exercising their [First Amendment](#) rights on matters of public concern.

Employees are to maintain an appropriate, professional relationship with students at all times. Employees are strongly encouraged to block students from viewing personal information on employee personal websites, personal email accounts, or social media 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 and it has a negative impact on the employee's ability to perform his or her job as it relates to working with students or other employees, the employee will be subject to discipline up to and including dismissal. This section applies to all employees and student teachers working in the school system.

H. Use of Social Media and Third-Party Websites for Educational Purposes

The Board recognizes that numerous social media platforms, websites, and cloud-based applications are owned and managed by third-party vendors may play an important role in the educational process. Any employee who seeks to utilize a social media platform, third-party website or cloud-based application, not under the Cabarrus County School domain, for instructional purposes, shall notify his/her principal or designee and shall attach the principal or designee to the account as an end user. In addition, prior to creating unique accounts for student access, the teacher shall notify the students' parent/guardian. Exemptions shall be made for accounts that have been prequalified by the CCS Chief Technology Officer or designee.

I. 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.

J. Consequences

Based on the nature and severity of the offense and the circumstances surrounding the incident, violations of this policy will result in appropriate remedial actions or discipline up to and including long-term suspension for students and dismissal for employees and may result in revocation of user privileges. Willful misuse may also result in criminal prosecution under applicable state and federal law.

Legal References: [U.S. Const. amend. I](#); Children's Internet Protection Act, [47 U.S.C. 254\(h\)\(5\)](#); [47 C.F.R. 54.516](#); 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. 6777](#); [G.S. 115C-47\(70\)](#), [-102.10 -325\(e\)](#) (applicable to career status teachers), [-325.4](#) (applicable to non-career status teachers); [143-805](#)

Cross References: Curriculum and Instructional Guides/Frameworks for Instruction (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), 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 Use of Social Networking Sites, Blogging and the Internet (Policy 4313), Use of Electronic Devices (Policy 4318), 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), 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

Adopted: August 10, 2009;

Revised: August 13, 2012; May 13, 2013; November 10, 2014; September 14, 2015; April 16, 2018; August 13, 2018; April 20, 2020; June 14, 2021; February 10, 2025; November 10, 2025; March 16, 2026; July 13, 2026.

Cabarrus County Schools