TECHNOLOGY RESPONSIBLE USE ***Policy*: 3225/4312/7320**

The Guilford County Board of Education 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 District'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 any technological resources owned, leased, maintained, or otherwise controlled by the District. This policy applies regardless of whether such use occurs on or off District property, and it applies to all District technological resources, including but not limited to computer networks and connections, the resources, tools, and learning environments made available by on or off the networks, and all devices that connect to those networks.

A. **Expectations for Use of School Technological Resources**

The use of District technological resources, including access to the Internet, is expected to be exercised in an appropriate and responsible manner. Individual users of the District's technological resources are responsible for their behavior and communications when using those resources. Responsible use of District 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.

Use, display, and possession of wireless communication devices issued by the school system shall be governed by section E. of this policy, as well as regulation 4300-R(1), Code of Conduct. General student and employee behavior standards, including those prescribed in applicable Board policies, the Student Code of Conduct, and other regulations and school rules, apply to use of District technological resources, including access to the Internet. In addition, anyone who uses District computers or electronic devices, accesses the school's electronic storage or network, or connects to the Internet using District-provided access 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. All students must be trained about appropriate online behavior as provided in policy 3226/4205, Internet Safety.

B. **Rules for Use of School Technological Resources**

1. District 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 District technological resources for commercial gain or profit is prohibited. Student personal use of District 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 District business, and is not otherwise prohibited by Board policy or procedure.

School system Wi-Fi hotspots and/or services may be used off school system property only by students and school staff members who need them. Such use must be primarily for activities that are integral, immediate, and proximate to the education of students.

2. Unless authorized by law to do so, users may not make copies of software purchased by the District. Under no circumstance may software purchased by the District 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 Student Code of Conduct.
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, violent, or considered to be harmful to minors.
6. Users must not circumvent fire walls. 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.
   a. Students must not reveal any personally identifying, private, or confidential information about themselves or fellow students when using email, chat rooms, blogs, 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 District 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.

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

d. Students may not use District 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 District 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 District-owned or issued devices.
11. Users may not create or introduce any foreign program or software, including games, network communications programs, or any foreign program or software onto any District computer, electronic device, or network without the express permission of 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.
13. Users are prohibited from using another individual's ID or password for any technological resource or account 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., 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, District administrator, or the technology director 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 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 District-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, technology director, or designee for the use of such devices.

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, District 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 or designee shall ensure that technology protection measures are used, 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**

Students, employees, visitors, and other users have no expectation of privacy in anything they create, store, send, delete, receive, or display when using the District's network, devices, Internet access, email system, or other technological resources owned or issued by the District, 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 District technological resources or stored on servers, the storage mediums of individual devices, or on school managed cloud services will be private. 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.

The District may, without notice, (1) monitor, track, and/or log network access, communications, and use; (2) monitor and allocate fileserver space; 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 District, 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 District from liability, and complying with public records requests. District personnel shall monitor online activities of individuals who access the Internet via a school-owned device.

By using the District's network, Internet access, electronic devices, email system, devices, or other technological resources, individuals consent to have that use monitored by authorized District personnel as described in this policy.

E. **Use of Personal Technology on School System Property**

Users may not use private Wi-Fi hotspots or other personal technology on campus to access the Internet outside the District's wireless network.

The Student Code of Conduct will restrict the use, display, and access to personal wireless communication devices during instructional time except as authorized by a teacher for educational purposes, in the event of emergency, if required by a student's Individualized Education Program or Section 504 Plan, or to manage a student's health needs.

~~Use of personal technology devices is also subject to any rules established by the superintendent.~~In addition to any disciplinary consequences described in the regulation 4300-R(1), Code of Conduct, ~~violations of this prohibition may result in the device being confiscated and only returned to the student's parent/caregiver.~~ The school system assumes no responsibility for personal technology devices brought to school. The Superintendent or designee may establish additional rules governing use of personal technology on school system property.

F. **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 District or individual school names, logos, or trademarks without permission.

1. Students

Though District personnel generally do not monitor students' Internet activity conducted on non-District 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 to the extent consistent with law (see the student behavior policies in the 4300 series).

2. Employees

Employees' personal websites (e.g. social media accounts) are subject to regulations issued by the superintendent. Employees may not use their personal websites to communicate with students, as prohibited by policy 4040/7310, Staff-Student Relations.

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 District may be terminated if the volunteer engages in inappropriate online interaction with students.

G. **Use Agreements**

All students, parents, and employees will be informed annually of the information in this policy. Prior to using District technological resources, students and employees must agree to comply with the requirements of this policy and consent to the District'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 District.

H. **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); 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); 143-805

Cross References: Staff-Student Relations (policy 4040/7310), Student Behavior Policies (all policies in the 4300 series), Student Records (policy 4700), Public Records (policy 5070/7350), Staff Responsibilities (policy 7300)

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

Replaces: EFE (adopted October 30, 2003)

Adopted: February 8, 2022

Revised: August 12, 2025; [date]