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~~ support diverse learning needs, ~~and~~ improve communication within the school community and ~~with the larger global community~~ beyond, 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. Users should take an active role in achieving their learning and teaching goals; model safe, legal and ethical behavior in digital environments; use effective digital research strategies, solve problems creatively; and collaborate with others to broaden their perspectives.

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~~school system~~ technological resources owned, leased, maintained, or otherwise controlled by the school system. This policy also applies to any non-students who are expressly authorized by the Wake County Public School System to use electronic information resources, including, but not limited to, Board of Education members, contractors, consultants, and temporary workers. 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, including access to the internet.

In addition, anyone who uses school system computers or electronic devices, ~~or who~~ accesses the school's electronic storage or network, or connects to the Internet using school system-provided access ~~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, a~~A~~ll students must be trained about appropriate online behavior.~~ All students receive digital literacy instruction, including digital citizenship and appropriate online behavior.

~~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 sign a statement indicating that they understand and will strictly comply with these requirements and acknowledging awareness that the school system may use 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 misuse may result in disciplinary action and/or criminal prosecution under applicable state and federal law.~~

B. RULES FOR USE OF 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. In addition, student access to social media platforms is prohibited, except when expressly directed by a teacher solely for educational purposes.

   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. The use of personal taglines or signature additions are not allowed on WCPSS email or other accounts.

   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. Using Wake County Public School Systems computers, networks, or other technology resources to endorse or oppose referendum, election, or particular candidate for office, including but not limited to advocacy in support of or against school bond referenda or candidates for the Board of Education is prohibited.

3. 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.

4. ~~Students and employees~~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 and

must follow any district applicable software application subscription service terms and conditions. ~~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.

5. Users must follow any software, application, or subscription services terms and conditions of use.

6~~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, or intended to and likely to incite imminent unlawful action, or otherwise prohibited by Board policy.

7~~6~~. Users must not circumvent network security measures (i.e. firewalls, etc.). The use of anonymous proxies to circumvent content filtering is prohibited.

8~~7~~. Users may not install or use any Wake County Public School System computer, network, or other technology resource to facilitate the sharing of copyrighted material.

9~~8~~. Users of technological resources may not send electronic communications fraudulently (i.e., by misrepresenting the identity of the sender).

10~~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 ~~W~~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~~ Such information includes, for example, a person's home address or telephone number, credit or checking account information, or social security number~~ of themselves or fellow students~~.

   b. ~~In addition, s~~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).

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

~~a.~~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. Additional exceptions will be made when recordings are used solely for classroom instruction or academic activity.

1~~0~~1. 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.

1~~1~~2. 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.

1~~2~~3. 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, data, or information.

1~~3~~4. Sharing Computer/Application Credentials: Users are prohibited from working under another person's login information (username and password). Users are prohibited from giving their login information to someone else or directing one to share their login information.

1~~4~~5. Users may not read, alter, change, block, execute, or delete files or communications belonging to another user without the owner's express prior permission.

1~~5~~6. Employees shall not use passwords or user IDs for any technology resource (e.g., the state student information and instructional improvement system applications, time-keeping software, etc.) for an unauthorized or improper purpose.

1~~6~~7. If a user identifies or encounters an instance of unauthorized access or another security ~~problem on a technological resource~~concern, he or she must immediately notify a teacher, ~~an~~school system administrator, or the technology director or designee. Users must not ~~demonstrate~~ share the problem ~~to~~ with other users. Any user identified as a security risk will be denied access.

18. It is the user's responsibility to back up data and other important files using approved local shared drive or cloud-based storage provided through the district.

19~~7~~. ~~Teachers~~ Employees shall make reasonable efforts to supervise students' use of the Internet during instructional time.

20~~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.

21~~19~~. Students may not access chat rooms unless assigned by a teacher or administrator for a valid educational purpose.

22. 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.

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 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~~users who connect to the Internet via their personal mobile technology~~.

~~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 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 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.~~

D~~E~~. PRIVACY

The Board intends that students and employees benefit from these resources while remaining within the bounds of safe, legal, and responsible use. 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, 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 school system 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 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 may monitor online activities of individuals who access the Internet via a school-owned device subject to policy 1710/4021/7230 Prohibition against Discrimination, Harassment, and Bullying.

In the course of monitoring the online activities of individuals who access the Internet as described in this policy, school system personnel may identify information pertaining to school safety or student safety. School system personnel who receive notice of online communications that suggest a student may be at imminent risk of harm should refer the matter to the student's family and/or appropriate authorities. However, parents and guardians must take primary responsibility for supervising and monitoring the online activities of their children when those activities occur outside of the school setting. The school system is not able to guarantee continuous, comprehensive monitoring of online activities such that it can identify and respond to potential risks suggested by various forms of online communication.

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

E~~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. Use of personal technology devices is also subject to expectations defined in Policy 4318 governing the Student Use of Personal Wireless Communication Devices. ~~any rules established by the superintendent or designee.~~ The school system assumes no responsibility for personal technology devices brought to school.

Students are expected to comply with the Code of Conduct and the applicable "Rules for Use of Technology Resources" set forth in this policy when students use a personal device on school property, at school sponsored events, on school-based transportation, or anytime a personal device is connected to school system technology resources. As an example, students using a personal device on school property, at school sponsored events, on school-based transportation, or when the device is connected to school system technology resources, shall not 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, or abusive.

F~~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 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.

2. Staff and Volunteers

Staff and volunteers are to maintain ~~an~~ appropriate relationships with students at all times. They are encouraged to block students from viewing personal information on personal websites or online networking profiles in order to prevent the possibility that students could view materials that are not age-appropriate. An individual staff or volunteer's relationship with the school system may be terminated if they engage in inappropriate online interaction with students as referenced in policy 4040/7310 Staff-Student Relations.

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~~.

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.

I~~H~~. WARRANTY

The school system makes no warranties of any kind, whether expressed or implied, for the technology services it is providing. The school system is not responsible for any damage suffered, including, but not limited to, loss of data resulting from delays, non-deliveries, miss-deliveries, service interruptions, or personal errors or omissions. Use of any information obtained via the Internet is at the user's risk. The school system specifically denies any responsibility for the accuracy or quality of information obtained through Internet access.

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

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

Adopted: July 21, 2015

Revised: March 5, 2019

Revised: December 7, 2021