Adopted: May 18, 2023

North Carolina Cyber Academy Board Policy
Technology Responsible Use

The Board 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 also applies to any non-students who are expressly authorized by North Carolina Cyber Academy 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. School Issued Google Accounts

NCCA will create a Google account for each student and staff member, which will be used along with the student or staff name to create accounts necessary for access to technology and digital resources. An NCCA school issued Google account may be visible in various applications to teachers and students across the system.

B. Laptops & Other Devices

North Carolina Cyber Academy (NCCA) uses a variety of technology and digital resources to enable and enhance instruction. With permission, students may use physical devices, including but not limited to, computers, tablets, and other hardware, for approved educational uses. All technology involves some sort of Internet access, herefore, technology access also means Internet access.

NCCA strives to provide a laptop computer or other physical device to every student for approved educational uses. All NCCA-issued devices may be inspected by NCCA officials, with or without prior notice, either in person or remotely via the Internet, for purposes of maintenance and/or to monitor the Student's use of the device (including any email and Internet activities) to determine whether the Student is complying with applicable laws, policies, and regulations. Students and parents have no reasonable

expectation of privacy to any data or information of any kind that is stored in a NCCA device, which remains at all times the property of NCCA. If any such inspection reveals that the Student has violated any provision of the NCCA District Handbook or any criminal law, any such evidence may be used in support of a disciplinary action against the Student and/or shared with law enforcement consistent with applicable law.

Parents who do not want their student to be issued a NCCA device may opt to provide their own for the student's use at school, so long as the device is a laptop computer (no tablets), has the latest operating system, and includes a keyboard, camera, and microphone. The device must otherwise be safe, adequate, and compatible with NCCA educational services and technology resources.

Any non-NCCA device that students use at school for educational purposes as an alternative to using a NCCA-issued device are subject to inspection and monitoring by NCCA at any time in the same manner and under the same circumstances as a NCCA-issued device. The fact that the device is private property does not insulate it from inspection and monitoring. Students and parents who do not wish their personal devices to be subject to monitoring and inspection at school have the option to use a NCCA-issued device instead.

C. Internet Safety Program for Students and Staff

NCCA has several processes in place to protect students and staff while using technology and web-based instructional tools. All students and staff will be required to be trained annually in Internet safety. In accordance with federal law, NCCA administration shall communicate and enforce an Internet-safety training program for all students under their care and all staff employed by the district. At a minimum, student training must include appropriate online behavior; interacting with other individuals on social media and in chat rooms and; cyber bullying awareness and response. The NCCA Technology and Innovation Department will maintain records that support the existence of the Internet Safety Program and how the program is implemented at NCCA.

D. Expectations for Use of School Technological Resources

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 NCCA District Handbook, 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 D below. These rules are intended to clarify expectations for conduct but should not be construed as all-inclusive.

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.

E. 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. 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 NCCA email or other accounts.
2. Using North Carolina Cyber Academy 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 is prohibited.
3. Under no circumstance may software purchased by the school system be copied for personal use.
4. Students and employees must comply with all applicable laws, 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 NCCA District Handbook.
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.
6. Users must not circumvent network security measures (i.e. firewalls, etc.). The use of anonymous proxies to circumvent content filtering is prohibited.
7. Users may not install or use any North Carolina Cyber Academy computer, network, or other technology resource to facilitate the 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. 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. 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 (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). Users also may not forward or post personal communications without the author's prior consent.
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.
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.
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. Sharing Computer/Application Credentials:
14. 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.
15. Users may not read, alter, change, block, execute, or delete files or communications belonging to another user without the owner's express prior permission.
16. 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.
17. If a user identifies a security problem on a technological resource, he or she must immediately notify an administrator. Users must not demonstrate the problem to other users. Any user identified as a security risk will be denied access.
18. Teachers 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. Students may not access chat rooms unless assigned by a teacher or administrator for a valid educational purpose.

F. Web-Based Applications

With the approval of an authorized NCCA teacher or administrator, students may access web-based applications to create, review, store, share and potentially post their work on the Internet. Examples of these tools include, but are not limited to the Canvas learning management system, productivity tools and GMail. NCCA has a review process, implemented in 2023- 2024, for web-applications, and approved applications must have acceptable security and privacy practices. Staff and students should only use applications that have been approved. Also of note, not all tools are used at all grade levels.

All NCCA business conducted online must utilize NCCA authorized communication programs or services. Those wishing to use third-party services must be approved by the Technology and Innovation Department so that the appropriate provisions may be added to the contract e.g., procedures, and contacts for public information requests.

G. 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 harmful to minors, including violence, nudity, or graphic language that does not serve a legitimate pedagogical purpose. The Board is not responsible for the content accessed by users who connect to the Internet via their personal mobile technology.

The district also uses Internet filters to remove most harmful content. District supplied devices and hotspots provide filtering at school and at home. These protective measures do not relieve students of their responsibility to comply with all applicable policies and procedures and to use school system technology and networks safely, responsibly, and in compliance with all applicable laws. Nor do they relieve parents and guardians of their responsibility to monitor and supervise safe and appropriate use of technology and the Internet in settings outside of school. Students are strictly prohibited from taking any measures to evade, disable, or circumvent any NCCA Internet filters or other NCCA technology protocols or procedures designed to protect the safety of students, NCCA technology resources, and/or the general public.

H. 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.

I. 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 will be private. The school system may, without notice, (1) monitor, track, and/or log network access, communications, and use; (2) and 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 may monitor online activities of individuals who access the Internet via a school-owned device subject to policy.

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, email system, devices, or other technological resources, individuals consent to have that use monitored by authorized school system personnel as described in this policy.

J. Use of Personal Technology on School System Property or at School Sponsored Events

The school system assumes no responsibility for personal technology devices brought to an NCCA sponsored event, testing site, or used to access NCCA resources.

Students are expected to comply with 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.

K. 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 the 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.

2. Staff and Volunteers
   Staff and volunteers are to maintain an appropriate relationship with students at all times. They are encouraged to block students from viewing personal information on personal websites or online networking profiles and social media 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.

L. Student Data

Student work and identifying information about students, such as name and classroom, may be maintained by and stored on web-based instructional sites and applications and/or on the NCCA server consistent with applicable law

M. 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); 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-325(e) (applicable to career status teachers), -325.4 (applicable to non-career status teachers)

15 U.S.C. § 6501 *et seq.*; 16 C.F.R. Part 312; 47 U.S.C. § 254; 18 U.S.C. § 2510 *et seq.*; 20 U.S.C. § 1681 *et seq.*; 20 U.S.C. § 1232g; G.S. 14-196.3; G.S. 15A-286 to 287; G.S. 115C-47(33); G.S. 115C-391; G.S. 115C-398; G.S. 115C-401.1; G.S. 115C-402; G.S. 115C-523