363.2-Rule

NORTH CAPE SCHOOL DISTRICT

STUDENT ACCEPTABLE USE OF TECHNOLOGY RULES

A. GENERAL EXPECTATIONS

The District's technology resources, including the District's technology-related equipment, software, networks, network connections, and Internet access, are open to limited and regulated use by students as a privilege. Each student who uses the District's technology resources is required to follow the District's established expectations for acceptable use.

In general, "acceptable use" means that a student is required to use technology resources in a manner that:

1. has a legitimate educational or other school-authorized purpose;
2. is legal;
3. is ethical (including, for example, avoiding plagiarism);
4. avoids harm to any person (including, for example, making threats, harassing or bullying someone, violating someone's privacy, accessing another person's accounts, records or files, etc.);
5. avoids harm to property (including, for example, damaging hardware, software, equipment, another person's work or electronic files, etc.);
6. avoids accessing or transmitting harmful or inappropriate material;
7. is respectful of others; and
8. is consistent with all applicable school policies, rules, and regulations, as well as any additional directives or instruction that may be provided by District staff.

Students should approach their use of technology resources with the understanding that all of the school rules and expectations that apply to in-person interactions and to the student's general conduct while at school or while under the supervision of a school authority also apply to their use of District technology, their online conduct, and their electronic communications. This document and various other District policies, rules and regulations include additional requirements and expectations that are directly related to the use of technology resources and electronic devices.

Policies, rules, and regulations cannot directly address every situation that a student may encounter. Therefore, an additional aspect of "acceptable use" is that the District expects each student who uses District technology resources to take an appropriate degree of personal responsibility for exercising sound judgment in his/her use of technology and in his/her technology-related activities and communications.

If a student has a question concerning any policy, notice, rule, regulation or directive that relates to technology resources, or if a student encounters a situation in which they are uncertain about any expectation for acceptable use or about how to proceed, the student should contact a teacher or the Technology Coordinator to obtain appropriate guidance

B. NOTICES TO STUDENTS WHO USE SCHOOL DISTRICT TECHNOLOGY RESOURCES

1. The District owns, controls, and oversees all of the school's technology resources, including the District's technology-related equipment, software, applications, networks, network connections, and Internet access. While present at school, all Internet or network access shall be accomplished solely and exclusively through District-provided Internet access. Should a student possess a device capable of accessing the Internet or network through a third-party source, the student must deactivate such device capability while at school and only access the Internet or network through District-provided resources.

2. Unless otherwise prohibited by law, at all times and without further notice:

    a. Each user of District technology resources is subject to direct and regular District oversight of, and District access to, any and all data, files, communications, or other material that the user creates, stores, sends, deletes, receives or displays on or over the District's Internet connection, network resources, file servers, computers or other equipment;
    b. All aspects of any individual's use of the District's technology-related equipment and resources, including any online activities that make use of District-provided Internet access, are subject to monitoring and tracking by District officials.

3. Except as to any privacy rights that independently exist under state or federal law, no person who accesses and uses the District's electronic networks and other technology-related equipment and resources does so with an expectation that any privacy right exists that would prevent District officials from (a) monitoring the person's activities; or (b) accessing any user's equipment, data, communications, and other materials.

4. The District's technology system(s) are provided on an "as is, as available" basis. The District does not make any warranties, whether expressed or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system(s) and any information or software contained therein. The District does not warrant that the functions or services performed by, or that the information or software contained on the system will meet the system user's requirements, or that the system will be uninterrupted or error-free, or that defects will be corrected. Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third party individuals in the system are those of the providers and not the District. The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's technology system(s).

5. If a student uses District technology resources in a manner that violates the District's expectations for acceptable use, or any other established policy, regulation, rule, or directive, the student is subject to possible disciplinary action. Examples of possible consequences for improper use of technology include the following:

a. Suspension, restriction, or revocation of the privilege of use of District technology resources;
b. The imposition of academic consequences for academic-related violations;
c. Suspension and/or expulsion from school; and/or
d. Referral to law enforcement.

C. SPECIFIC ACCEPTABLE USE RULES

1. **Unauthorized Access and Other Prohibited Activities** – Students are prohibited from engaging in (or attempting to engage in) the following conduct at all times:

   a. Using the District's technology resources or system(s) for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy.
   b. Knowingly accessing educationally inappropriate material. If a user accidentally reaches such material, the user must immediately back out of the area on the Internet containing educationally inappropriate material. The user must then notify the teacher or other District staff person of the site address that should be added to the filtering software, so that it can be removed from accessibility.
   c. Using another person's login or password information; or allowing another person to use the student's own login or password information. The user, in whose name a system account is issued, will be responsible at all times for its proper use.
   d. Uploading programs to the District's system without appropriate authorization. The Technology Coordinator is authorized to set limits for disk utilization on the system(s) as needed.
   e. Physically connecting any personally-owned technology equipment to a District network (including computers, laptops, tablets, smart phones, printers, etc.) except for (1) authorized connections to the wireless network the District provides expressly for students and guests, if any; and (2) temporarily connecting data drives/devices to District equipment for the purpose of transferring data or files for an educational or other authorized purpose.
   f. Disabling Internet tracking software or implementing a private browsing feature on District computers or networks. Browsing history shall only be deleted by authorized staff or in accordance with the District's technology department's directives
   g. Modifying without permission any District records, any District-controlled web pages or web-based accounts, or any of the District's Internet-based resources. Users will take all appropriate precautions
   h. Using District technology resources for any private commercial activities (for example, solicitations or advertisements) or for any activities that involve political advocacy connected to any election.

2. **Rules and Expectations Related to Copyright Law, Licensing Agreements, and Related Issues**

   a. While using the District's technology resources, students are individually responsible for following applicable laws, regulations, and agreements that relate to the use of any other person's or entity's products, services, or content.

b. Students may not use any electronic content, application, software, or technology service (1) that has not been properly purchased or licensed; or (2) in any manner that violates a license, user agreement, or the terms of use established by the owner/manufacturer/vendor of the product, service, or content.
c. Students may not redistribute copyrighted programs or data without the written permission of the copyright holder or designee. Such permission must be specified in the document or must be obtained directly from the copyright holder or designee in accordance with applicable copyright laws, District policy, and administrative regulations. Students are cautioned that the fact that an image, video, recording, article, file, program, book, or other work that is subject to copyright (or trademark protection) is available through the Internet does not mean that it is in the public domain (i.e., able to be freely used), or that it can be further used, copied, or adapted without first obtaining appropriate permission from the person or entity who holds the applicable rights.
d. Property created by a student that is submitted as an assignment or for an assessment, or for a grade or course credit, may be retained by the District as a student record and displayed for school purposes subject to laws and any District policy or procedures that govern such records. The District may further extend its right to retain, reproduce, distribute or otherwise use student-created intellectual property by obtaining specific permission from the student and the parent/guardian.
e. To the extent consistent with applicable law, the District retains the exclusive right to determine, at its discretion, the content that is permitted to be displayed or otherwise made available to the school community and/or to the general public through the District's technology resources.

3. **Rules and Expectations Related to Academic Integrity/Plagiarism**

a. District and individual teacher expectations regarding honesty and fairness in academic contexts apply fully to activities that involve the use of technology.
b. Students shall not plagiarize works that they find on the Internet. Plagiarism includes copying, close paraphrasing, or representing as one's own the writing, ideas, or other work of another person without appropriate attribution. Users will use proper bibliography formats.

4. **Electronic Communication by Students**

a. There are various forms of electronic communication that students may be able to access and use through the District's technology resources. Examples include course-management applications that permit student submissions, email, social media platforms, chat functionality, message boards, applications that function like text messaging, etc. While all social media is subject to the District's technology use policies, rules and restrictions, the following forms of social media are expressly approved by North Cape and it is the intention of the District to utilize these specific forms of social media to enhance the educational experience of students: Google in Education, Google in Education applications, YouTube Education, and North Cape's private YouTube Channel.

b. Students using District technology resources to engage in any form of electronic communication are expected to follow the District's rules and expectation for "acceptable use" as defined in this document, and, as far as the content and purpose of their electronic communications, students are expected to adhere to the school rules and expectations that apply to in-person interactions, including the Code of Classroom Conduct and North Cape PBIS Expectations Matrix.
c. The following are specific examples of conduct that is prohibited in connection with a student's use of District technology resources for electronic communications:
   (1) Electronic communications must not contain defamatory, discriminatory, threatening, offensive, racist, disrespectful, sexually-explicit, profane, or obscene content.
   (2) Electronic communications must not be used to bully, harass, degrade, or intimidate another person.
   (3) Electronic communications must not be used to facilitate any unlawful activity or any violation of school rules.
   (4) Students shall not engage in electronic communications with persons who are not affiliated with the District unless the communication is for a legitimate educational or other authorized purpose and the student is reasonably sure of the identity of the person or entity with whom they are communicating.
   (5) Students shall not post personal contact information about themselves or other people or any other information which is confidential or of a private nature. Personal contact information includes home and school addresses, telephone numbers, etc.
   (6) Students shall not agree to meet with someone they have met online without the approval of their parent(s)/guardian.
   (7) Students shall not attempt to access or send electronic communications using another person's account or user ID. Similarly, students shall not impersonate another person using electronic communications.
   (8) Students shall not create, transmit, or forward messages, Internet-links, images, files, or attachments that do not have a legitimate educational purpose (for example: spam, jokes, etc.) and/or that may be harmful (for example: executable files, viruses, requests for personal or confidential information, material from an unknown source, etc.).
   (9) Forgery or attempted forgery of electronic communications is prohibited.
   (10) Electronic communication received from another person should not be forwarded or shared gratuitously when the original sender has clearly indicated their intent that the message should not be forwarded or shared. This limitation is not intended to prevent a student from addressing a safety concern or reporting a violation of school rules by contacting a responsible adult.
   (11) Students shall not use any technology device capable of capturing video, pictures, or audio to record or take pictures of any other individual without their express consent and permission. No such recording or pictures shall be posted or communicated unless it is educationally related. Students are not allowed to "tag" an individual in a picture or recording without their express consent and permission.
d. Examples of acceptable electronic communications involving the use of District technology resources include:

(1) Communicating with a teacher regarding schedules, assignments, curriculum content, class projects, and class activities via the teacher's District-provided email or network account.
(2) Communicating with other students to facilitate collaboration, planning, and research for school-related projects and activities.
(3) When authorized by a teacher, communicating with third parties outside of the District as a means of collaborative learning, academic research, or other school-related purpose.

5. **Use of Personal Electronic Devices at School**

a. A student may bring a personal electronic device to school and use the device only to the extent consistent with this document, related Board policies (Policy 443.5 on Student Use of Personal Electronic Communication Devices and Policy 731.1 on Privacy in Locker Rooms), and any other rules or directives issued by the District or school staff to govern the time, place, and manner in which students may possess and use personal electronic devices.
b. Any student possessing a personal electronic device capable of accessing the Internet or network through a third-party source must deactivate such device capability while at school and only access the Internet or network through District-provided resources.
c. Personal electronic devices may be used in the classroom or during a student's participation in organized school activities if expressly allowed by the teacher or activity supervisor. As an important exception to all rules and directives that might otherwise limit a student's permission to possess and use a personal electronic device, all students at all grade levels may use a device (at any time of day) to contact a responsible adult in any emergency situation that involves an immediate threat to the health or safety of any person. When carrying out school emergency response plans, however, students may be asked to turn off their personal electronic devices so emergency communication networks are not overwhelmed and emergency response efforts are not jeopardized. When a staff member issues a specific directive or limitation related to the possession or use of any electronic device, students are expected to follow that directive/limitation.
d. The District assumes no responsibility for the loss or theft of, or for any damage to, any personal electronic device that a student chooses to bring to school or to a school activity regardless of (1) when the loss, theft, or damage occurs; or (2) where the device is located/possessed at the time the loss, theft, or damage occurs. The District is permitted, but not obligated, to investigate or otherwise resolve the loss or theft of, or any damage to, any personal electronic device.
e. Where the District has reason to suspect that any personal electronic device is present or has been used in violation of any Board policy or school rule, school personnel may temporarily confiscate the device. Staff shall make an effort to store a confiscated device in a reasonably secure location. To the extent consistent with applicable law, a confiscated device may be subject to a search by a school administrator or law enforcement officials.
f. Students are required to relinquish electronic devices to school personnel when directed. Refusal to comply or interfering with such a directive (e.g., by removing the battery or memory card without permission) will be considered insubordination and the student will be subject to disciplinary action.

6. **Reporting Student/Parent Concerns, Misuse, or Other Possible Violations of Acceptable Use**

    a. Any time a student feels unsafe, victimized, or in any way uncertain about a situation involving the use of District technology resources by any person, the student (or his/her parent(s)/guardian should immediately contact a teacher, the Technology Coordinator or the District Administrator.
    b. Students are required to report and provide to a teacher or other school official any electronic communication that they receive while using a District-provided email account, or using any District-provided electronic software, program, application or platform if any of the following apply:
        (1) The communication is from an unknown source and either contains inappropriate content, asks the student to respond, or requests the student to reveal personal information;
        (2) The content of the communication is defamatory, discriminatory, threatening, offensive, racist, deceptive, sexually explicit, or obscene;
        (3) The communication represents an attempt to bully, harass, or intimidate another person; or
        (4) The content of the communication represents an attempt to facilitate or encourage any violation of the law or school rules.
    c. A student may report to any teacher, the Technology Coordinator or the District Administrator any concerns about possible violations of the policies, rules, regulations and directives that govern the acceptable, safe, and responsible use of the District's technology-related resources.
    d. If a student has a concern that any District technology equipment, network, or system may have a security vulnerability, or that any breach of security may have occurred, the student shall report the issue to a teacher or to the Technology Coordinator. The student should not demonstrate the potential security problem to anyone other than to the person to whom they report the concern.
    e. If a student or parent/guardian has a concern that any content that is available through the Internet is (1) appropriate material that is currently being blocked or filtered, or (2) harmful or inappropriate material that is not being blocked or filtered, the individual may report that concern to the District Administrator or Technology Coordinator. The District will review the issue and report back to the person making the report.

REVISION AND NEW APPROVAL: January 16, 2017