



CHEROKEE COUNTY SCHOOL DISTRICT

Mobile Computing Guide 2018-2019

Cherokee County School District provides this guide so that students and their parents/guardians can become familiar with the district's Personal Mobile Computing initiative. It contains a brief overview of the initiative, frequently asked questions, forms and other information.

In May 2013, the Cherokee County School District Board of Trustees approved a visionary new mobile learning initiative to transform teaching and learning in and out of the classroom. Cherokee County School District will equip every student in grades 2-12 with a touch screen laptop. Grades 4K – 1 will receive an iPad.

T2- Technology Transforms CCSD, the district's 1:1 mobile learning initiative, is focused on preparing students with 21st Century skills they will need to be successful in postsecondary education and their careers. In addition to the content students learn in math, science, English, and social studies, it is critical they become proficient in communication, collaboration, critical thinking, and creativity as featured in the Profile of a S.C. Graduate.

1:1 mobile technology addresses these skills by providing students with a powerful educational tool that not only raises engagement and excitement for learning, but also provides them access to the vast global network of information available online. 1:1 mobile technology allows a more personalized learning experience where instruction can address higher order thinking, mastery and self-paced learning, all while focusing on critical skills like research, writing, and content development.

Recognizing the need to prepare teachers for this significant shift in learning delivery, the district continues to train teachers in accordance with the strategic plan.

Student online safety will be a priority in every stage of implementation. All mobile devices must access the Internet through our district's web filter, blocking any inappropriate content. Even when students access the Internet on their devices away from school, all web use will run through the district's filter. Additionally, only teacher recommended, district-approved apps or programs will be installed on students' devices.

As increasing numbers of students have personal cell phones and tablets that provide quicker accessibility to learning opportunities than standard desktop computers, it is essential that schools keep pace with this technology revolution, or we risk becoming obsolete learning institutions. We are proud that our Board of Trustees supports our district continuing to be a front runner in instructional technology.

Sincerely,

A handwritten signature in cursive script that reads "Quincie L. Moore".

Quincie Moore
Superintendent

TABLE OF CONTENTS

LETTER FROM THE SUPERINTENDENT	1-2
RECEIVING/RETURNING YOUR MOBILE COMPUTING DEVICE	5
Distribution of Mobile Computing Devices	
Returning Mobile Computing Devices	
Identification of Mobile Computing Devices	
CARING FOR THE MOBILE COMPUTING DEVICE	6
General Precautions	
Carrying Mobile Computing Devices	
Screen Care	
USING YOUR MOBILE COMPUTING DEVICE	7-10
Mobile Computing Devices Left at Home	
Mobile Computing Device Undergoing Repair	
Charging Your Mobile Computing Device's Battery	
Printing	
Home Internet Access Camera Use	
MANAGING YOUR FILES AND SAVING YOUR WORK.....	10
Saving to the Network Home Directory	
Network Connectivity	
APPLICATIONS ON MOBILE COMPUTING DEVICES	10-11
Originally Installed Applications	
Additional Applications	
Inspection	
Procedure for Reloading Applications	
Application Upgrades	
DIGITAL CITIZENSHIP	11-12
District Responsibilities	
Student Responsibilities	
Parent/Guardian	
Responsibilities Creative Commons	
Copyright Mobile	
Computing Device Care	
MOBILE COMPUTING DEVICE DAMAGE OR LOSS	12-13
Terms of the Mobile Computing Device Agreement	
Title	
Repossession	
Liability	
APPENDIX A.	14
Mobile Computing Device Agreement (<i>Parent/Guardian Signature</i>)	

APPENDIX B	15
Student Pledge for Use of the Mobile Computing Device (<i>Parent/Guardian Signature</i>)	
APPENDIX C	16-22
Cherokee County School District Acceptable Use Policy	
APPENDIX D	23-26
Cherokee County School District Mobile Computing Device Discipline	
Plan for Middle and High	
APPENDIX E	27
Cherokee County School District Mobile Computing Device Discipline	
Plan for Primary and Elementary	

* *References to trademark and brand ownership have been removed for ease of reading but, in all cases, should be taken as read and respected.*

RECEIVING/RETURNING YOUR MOBILE COMPUTING DEVICE

Distribution of Mobile Computing Devices

Mobile Computing devices will be distributed each year following each school's Mobile Computing Device Orientation.

Families with more than one child will be eligible for a reduced rate for the annual technology fee.

Returning Mobile Computing Device

Students transferring out of or leaving Cherokee County School District during the school year must return the Mobile Computing device (including power cords, and any other district- or school-issued accessories) before leaving the school.

Seniors will return their Mobile Computing devices (including power cords, and any other district-or school-issued accessories) to the high school before graduation.

If a student does not return his/her Mobile Computing device upon leaving the district, the parent/guardian will be required to pay the replacement cost for a new device. Failure to pay for a device will subject the parent/guardian to legal liability.

If a student returns his/her Mobile Computing device damaged maliciously, costs for replacement or repairs are the parent/guardian's responsibility. The district will charge the parent/guardian the cost of needed repairs, not to exceed the replacement cost of the device.

Identification of Mobile Computing Device

Each student's Mobile Computing device will be labeled in the manner specified by the district. Mobile Computing devices can be identified by Serial Number as well as Cherokee County School District Inventory Label.

CARING FOR THE MOBILE COMPUTING DEVICE

The Mobile Computing device is district property. All users will follow these guidelines and the Cherokee County School District Acceptable Use Policy for technology.

Students are responsible for the general care and maintenance of their school-issued Mobile Computing device.

Students are responsible for any and all damage to their device.

Students must take any damaged Mobile Computing devices or devices failing to operate properly to the Tech Center who will forward it for evaluation and/or repair. Cherokee County School District will be responsible for repairing devices that malfunction.

General Precautions

Carefully insert cords and cables into the Mobile Computing device to prevent damage.

Mobile Computing devices must remain free of any writing, drawing, stickers or labels that are not the property of Cherokee County School District.

Never leave your Mobile Computing devices in an unlocked classroom, locker, car, or any other unsupervised area.

Students are responsible for keeping their Mobile Computing device's battery charged for school each day.

Carrying Mobile Computing Devices

Students must keep their Mobile Computing devices secure at all times.

Devices should be kept in the protective cases provided and a carried in a book bag or separately to avoid placing excessive pressure and weight on the Mobile Computing device screen.

Screen Care

Screen damage may occur when pressure is applied to the screen. Users must avoid leaning on the top of the device or placing objects in a book bag or protective case in a way that it applies pressure to the screen.

Use only a dry soft cloth or anti-static cloth to clean the screen. Do not use cleansers of any type.

Do not bump the Mobile Computing device against hard surfaces, e.g. lockers, walls, car doors, floors, etc., as it may break the screen.

USING YOUR MOBILE COMPUTING DEVICE

Mobile Computing devices are intended for use at school each day. Students are responsible for bringing their Mobile Computing device to all classes (except PE), unless specifically instructed otherwise by a teacher.

In addition to using their device for classroom learning activities, students may also access school messages, announcements, calendars, and schedules.

Mobile Computing Devices Left at Home

Students who leave their Mobile Computing device at home are still responsible for completing their daily course work. Repeated offenses may result in disciplinary action, as outlined in Appendix D.

Mobile Computing Devices Undergoing Repair

The school may issue a loaner Mobile Computing device to a student while his/her device is being repaired by staff. There may be a delay depending upon availability of a loaner Mobile Computing device.

Charging Your Mobile Computing Device's Battery

Mobile Computing devices must be brought to school each day in a fully charged condition. Students must charge their Mobile Computing devices each evening. Repeat violations of not charging the battery for the school day may result in disciplinary action as outlined in Appendix D.

Printing

Students can print from their Mobile Computing devices in designated areas.

Schools will give students information about printing with their Mobile Computing devices while at school.

Home Internet Access

Students may establish Wi-Fi connections with their Mobile Computing devices outside of school. Students can then use their device wherever access is available.

Camera Use

The district-owned device comes equipped with a front-facing camera and video capabilities. **The use of a camera in restrooms, locker rooms, or on the bus is strictly prohibited.** The district reserves the right to remove access to the camera at any time.

The Family Educational Rights and Privacy Act (FERPA) is a federal law that affords parents and students over 18 years of age certain rights with respect to student privacy and educational records, including photographs. **For this reason, students must obtain permission to**

publish or make publicly available a photograph or video of any school- related activity. Unauthorized recordings are subject to disciplinary action in accordance with the district's *Acceptable Use Policy* (Appendix C). Cherokee County School District retains the rights to any recording and/or publishing of any student's or staff member's work or image.

Additional information about FERPA can be found in the forms and notices packet distributed at the beginning of school, on the district website, and/or online at www2.ed.gov/ferpa.

Device Rules and Guidelines

The rules and regulations are provided here so that students and parents/guardians are aware of the responsibilities students accept when using a district-owned device. In general, this requires efficient, ethical, and legal utilization of all technological devices. Violations of these rules and guidelines will result in disciplinary action. Students will receive device-related training at school on proper use and digital citizenship.

Below is a review of the rules and guidelines:

Electronic Resource Policy and Responsible Use Procedures All Use of Technology Must

- Support learning.
- Follow local, state, and federal laws.
- Be school appropriate.

Security Reminders

- Do not share log-ins or passwords unless asked to do so by a parent/guardian or school personnel.
- Do not develop programs to harass others, hack, bring in viruses, or change others' files.
- Follow Internet Safety guidelines.

Activities Requiring Teacher Permission During Instructional Time

- Playing content-related games
- Sending email
- Using headphones in class, where related
- Use of camera for pictures or video

Activities PROHIBITED on School Property

- Instant-messaging (e.g., Face Time, SnapChat, KIK, Yik Yak, etc.)
- Playing non-educational games
- Downloading programs, music, games, and/or videos
- Using a Hot Spot with a district-owned device

Inappropriate Content-All files must be school appropriate. Inappropriate materials include explicit or implicit references to

- alcohol, tobacco, or drugs
- gangs
- obscene language or nudity
- bullying or harassment
- discriminatory or prejudicial behavior
- illegal activities

Student-Email Purpose

All students are issued an email account. Email allows students to safely and effectively communicate and collaborate with staff and classmates, giving them an authentic purpose for writing. Effective use of email is

- a 21st Century communication tool.
- used in careers and higher education settings.

Guidelines and Reminders

- Email should be used for educational purposes only.
- Email transmissions may be monitored by the school at any time to ensure appropriate use: any school personnel may check students' email.
- All email(s) and its/their contents are the property of the district.
- Email should be used only by the authorized owner of the account.
- Students need to protect their passwords.

Unacceptable Use Examples

- Non-education-related forwards (e.g., jokes, chain letters, images, etc.)
- Harassment, profanity, obscenity, racist terms
- Cyber-bullying, hate mail, discriminatory remarks
- Email for individual profit or gain, advertisement, political activities, or illegal activities

Webcams Purpose

Each student device is equipped with a webcam. This equipment offers students an extraordinary opportunity to experience a 21st Century tool and to develop 21st Century communication skills.

Important Note

Cherokee County School District retains the rights concerning any recording and/or publishing of any student or staff member's work or image. Students must obtain permission to record, take, or publish a photograph or video of any person. Unauthorized recordings are subject to disciplinary action in accordance with School Board Policy.

Media/Music/Gaming

- Movies, music, games and other media should not interfere with the learning process.
- Streaming is not allowed because it creates district bandwidth problems. If a certain media is necessary for instructional purposes, it should be downloaded, not streamed.

Wallpaper

Any images set as the wallpaper must be in line with the Acceptable Use of Technology Resources Policy. Inappropriate media may not be used as wallpaper. Presence of guns, weapons, pornographic material, inappropriate language, alcohol, drugs, or gang-related symbols will result in disciplinary action.

Copyright and Plagiarism

Students are expected to follow all copyright laws. Duplication and/or distribution of materials of educational purposes is permitted when such duplication and/or distribution would fall within the Fair Use Doctrine of the United States Copyright Law.

MANAGING YOUR FILES AND SAVING YOUR WORK

Saving to the Network Home Directory

Students may save their work to their folder on the school's server via their home directory (H: drive) or to OneDrive, a type of cloud storage, since they will have limited storage space on their Mobile Computing devices.

OneDrive is based on the Hypertext Transfer Protocol (HTTP) that facilitates collaboration between users in editing and managing documents and files stored on World Wide Web servers.

Students will open files online to work on them and save them back to the cloud. It is each student's responsibility to ensure that his/her work is not lost due to mechanical failure or accidental deletion.

Mobile Computing device malfunctions should not be used as an excuse for failure to submit work.

Network Connectivity

Cherokee County School District makes no assurance that the network will be operational at all times. In the rare instance that the network may not be operational, the district will not be responsible for lost or missing data.

APPLICATIONS ON PERSONAL MOBILE COMPUTING DEVICES Originally Installed Applications

The applications originally installed by Cherokee County School District on each Mobile Computing device must remain on the device in usable condition and readily accessible at all times.

You may not remove these required applications, and staff will periodically check Mobile Computing devices to ensure that students have not removed them. The school may also add other applications periodically.

Some licenses for applications require that the application be deleted from the Mobile Computing device at the completion of a course. If this applies to an application students use, technology staff will re-image the devices of the students in that course.

Additional Applications

Cherokee County School District syncs Mobile Computing devices so that they contain the necessary applications for school work.

Students will be permitted to load additional applications on their Mobile Computing devices as long as they do so in accordance with the district's Acceptable Use Policy. You can read the entire Acceptable Use Policy in Appendix C.

Inspection

Staff may randomly select students and ask them to provide their Mobile Computing device for inspection.

Procedure for Reloading Applications

If technical difficulties occur, or unauthorized applications are discovered, technology staff will re-image the Mobile Computing device. The school does not accept responsibility for the loss of applications or documents from a re-image.

Application Upgrades

The district will distribute upgraded versions of licensed applications from time to time through network processes or manually by a technician.

DIGITAL CITIZENSHIP

Digital Citizenship is a concept which helps students, parents, and teachers, understand what these users should know to use technology appropriately. Digital Citizenship is not only a teaching tool, but also a way to prepare students/technology users for a society full of technology.

The district expects students to use technology appropriately and responsibly at all times.

The district has electronic security precautions to ensure that students participate safely and securely when using digital devices.

District Responsibilities

The school will provide Internet and e-mail access to students.

School staff will help students conduct research and ensure student compliance with the district's Acceptable Use Policy (see Appendix C).

Filtering/blocking of inappropriate Internet materials is done at the district level, and the district provides network or cloud data storage areas for all students.

Cherokee County School District reserves the right to investigate any inappropriate use of resources and to review, monitor and restrict information stored on or transmitted via Cherokee County School District owned equipment and resources.

Student Responsibilities

Students will abide by the district's **Acceptable Use Policy** (see **Appendix C**) and:

- contact an administrator about any security issue they encounter.
- monitor all activity on their personal account(s).
- always shut down and secure their Mobile Computing device after use to protect their work and information.
- report e-mail(s) containing inappropriate or abusive language or questionable subject matter to a teacher or administrator at school.
- return their Mobile Computing device to the school at the end of the school year or on the date they withdraw or transfer. (This also applies to seniors who graduate mid- year.)

Parent/Guardian Responsibilities

Parents/guardians should talk to their children about the values and standards they expect them to follow as they use the Internet just as they should do with all other media information sources such as television, telephone, movies, radio, etc.

When accessing the Internet away from school, all district-issued Mobile Computing devices will be re-directed to the district's filter. Parents are encouraged to monitor student activity at home, especially Internet access on the district and home devices.

Creative Commons Copyright

With student permission, a student's work may be uploaded to the internet and shared with others where appropriate for academic purposes.

Students own the copyright to their original literary and/or artistic works. Students will be encouraged to select one of the Creative Commons Copyright licenses to include with their work when uploading to the internet. This license will state how the work can be used by others.

All material and work created on the device are subject to review, and deletion by, district staff at any point in time if they are found to be in violation of the district's Acceptable Use Policy, and/or any state or federal laws.

The district is not responsible for the loss of any students' intellectual property whether it be because of technical issues, or because it was removed due to policy violations, and cannot be held liable for the loss of such material.

MOBILE COMPUTING DEVICE DAMAGE OR LOSS

Terms of the Mobile Computing Device Agreement

Terms and conditions that apply to the usage of the Mobile Computing Device under the Protection Plan are as follows:

- Parents must pay replacement cost for obvious malicious damage.
- Parents are responsible for lost/damaged power supplies. Costs of device and device accessories will be posted on the district web site.

Title

Legal title to the device shall remain with the district at all times.

The right of possession and use is limited to, and conditioned on, full and complete compliance with the Mobile Computing Device Agreement.

The student is responsible at all times for the mobile computing device's appropriate care and use.

Repossession

Cherokee County School District reserves the right to repossess any Mobile Computing device for failure to comply with all terms of the Mobile Computing Agreement.

Liability

Cherokee County School District reserves the right to demand return of the Mobile Computing device at any time. Mobile Computing device agreements are good for one year (from the first day of school until the last day of school), unless the agreement is terminated earlier.

Failure to return the Mobile Computing device to the school before departure from the district may result in legal action against the student and/or parent/guardian.

In the event of loss or vandalism away from school:

In the event a Mobile Computing device is lost, stolen, or vandalized away from school, the parent/guardian must report the loss or damage to the school immediately and file a police report within 48 hours. The parent/guardian must provide a copy of the police report to the principal.

In the event of theft or vandalism at school:

The student must report the loss or damage of the device to school administration immediately and ensure a police report is filed within 48 hours. The parent/guardian must provide a copy of the police report to the principal.

APPENDIX A: MOBILE COMPUTING DEVICE AGREEMENT

CCSD Mobile Computing Device Protection Plan

Cherokee County School District recognizes that with the implementation of the Mobile Computing Device Initiative, a major priority must be to protect the investment by the district and the parent/guardian.

The following information outlines the various aspects of protection: warranty and accidental damage protection.

The Annual Technology fee costs \$50 per school year for each Mobile Computing device. Families with more than one student will pay \$30 for each additional child. Students eligible for free and reduced benefits will receive a discounted technology fee rate.

Parents/guardians will be responsible for the entire cost of replacement/repair for Mobile Computing devices damaged through misuse, abuse, intentional damage. Parents/guardians will be responsible for the entire cost of a lost/stolen device (\$550).

Please note: This form will serve as your acceptance for each and every year your student receives a device.

CCSD Mobile Computing Device Protection Plan

Parent/Guardian Name (Please Print): _____ Date: _____

Parent/Guardian Signature: _____ Date: _____

Student Name (Please Print): _____ Date: _____

Office Use Only

Amount Paid: _____ Balance: _____ Cash: _____ Check: _____ Credit Card: _____

Accepted by: _____ Date: _____

APPENDIX B: STUDENT PLEDGE FOR USE OF THE MOBILE COMPUTING DEVICE

1. I will take proper care of the Mobile Computing device.
2. I will not loan the Mobile Computing device or charger and cords to others.
3. I will be accountable for the Mobile Computing device at all times.
4. I will charge the Mobile Computing device's battery daily.
5. I will not leave the Mobile Computing device in any unsupervised area.
6. I will keep food and beverages away from the Mobile Computing device.
7. I will not disassemble any part of the Mobile Computing device nor attempt repairs.
8. I will not remove district-required applications.
9. I will protect the Mobile Computing device by carrying it securely.
10. I will not stack objects on top of the Mobile Computing device.
11. I will not leave the Mobile Computing device outside or use it near water.
12. I will save data to the district-assigned cloud storage (Cherokee County School District will at times E-sync Mobile Computing devices. All files not saved to server or other storage media will be deleted during these processes. I am responsible for saving all my personal files).
13. I will not place decorations (such as stickers, markings, etc.) on the Mobile Computing device case.
14. I will not deface the serial number, manufacturer labels or district labels on any Mobile Computing device.
15. I will follow district policies outlined in the Personal Mobile Computing Guide and the Board's Acceptable Technology Use Policy.
16. I will notify my teacher or principal immediately in the event of theft, vandalism, or other damage of the device. If my device is lost or stolen, I will ensure that a police report is filed within 48 hours.
17. I will be responsible for all damage or loss caused by my neglect or abuse of the device.
18. I agree to return the Mobile Computing device and power cords in good condition.
19. I agree to return the Mobile Computing device and power cords when I transfer or leave the district for any reason. I understand that restitution will be sought legally if I fail to return the device.

By my signature (Student), I agree to the stipulations set forth above and the Board's Acceptable Use Policy. I understand my device is the property of Cherokee County School District and is subject to inspection at any time. By my signature (Parent/Guardian), I understand my responsibility for loss or intentional damage to the device. Also, I understand that I am responsible for any stolen device that is not recovered.

Parent/Guardian Name (Please Print): _____ Date: _____

Parent/Guardian Signature: _____ Date: _____

Student Name (Please Print): _____ Date: _____

Student Signature: _____ Date: _____

APPENDIX C: CHEROKEE COUNTY SCHOOL DISTRICT ACCEPTABLE USE POLICY

Policy IJNDB Use of Technology Resources in Instruction

Issued 6/13

Purpose: To establish the board's vision and the basic structure for the use of technology resources in instruction.

Internet access

Because technology is a vital part of the educational process and the curriculum of Cherokee County School District, students and staff will be provided access to the Internet when appropriate. By providing this access, the district intends to promote educational excellence in schools by facilitating resource sharing, innovation, communication and learning and by allowing access to resources unavailable through traditional means. Through the Internet, students and staff will have access to the following.

- locally networked reference and research sources
- global information and news
- local, regional, public, state and national library catalogs
- worldwide web
- electronic mail sources
- virtual classes

The availability of Internet access provides a unique educational opportunity for students and staff to contribute to the district's presence on the worldwide web. This medium of communication provides an opportunity to share accurate information with the community, the state and the world about the district's curriculum and instruction, school-authorized activities and other related information. The district provides this instructional resource as an educational tool for staff and the technology acceptable use policy will govern its uses. The failure to follow this policy may result in the loss of privileges or other disciplinary measures as outlined in JICDA-R.

With access to computers and people all over the world also comes the availability of material that may not be of educational value in the context of the school setting. The district has taken precautions to restrict access to controversial or inappropriate materials; however, on a global network it is impossible to control access to all materials, and an industrious user may discover controversial information. The district firmly believes that the valuable information and interaction available on this worldwide network far outweighs the possibility that users may procure material that is not consistent with the educational goals of the district. Users are responsible for reporting to the district's director of technology or his/her designee controversial or inappropriate websites they are able to access so the websites can be added to the district's filter. The smooth operation of the technology network relies on the proper conduct of the end users who must adhere to strict procedures. These procedures are provided so that students and staff are aware of their responsibilities when using the technology and the Internet. Any violations of these procedures will subject the user to appropriate disciplinary action and possible denial of access to the Internet. In general, this requires efficient, ethical and legal utilization of the network resources. Because access to the network provides connections to other computer systems located all over the world, users and parents/legal guardians of students who are users must understand that neither the district nor any district employee controls the content of the information available on all of these systems. The district does not condone the use of controversial or offensive materials and cannot be held responsible for such use.

Technology protection measures

In compliance with the Children's Internet Protection Act (CIPA), 47 U.S.C. § 254(h), the district uses technological devices designed to filter and block the use of any of the district's computers with Internet access to retrieve or transmit any visual depictions that are obscene, child pornography or "harmful to minors" as defined in the CIPA. The district will provide continuing education to students on acceptable and proper online behavior. The district will provide reasonable notice of and at least one public hearing or meeting to address and communicate its Internet safety measures.

Reporting

District and school computer technicians who are working with a computer and come across sexually explicit images of children must report this to local law enforcement. The report must include the name and address of the owner or person in possession of the computer.

Off-campus conduct

Students, parents/legal guardians, teachers and staff members should be aware that the district may take disciplinary actions for conduct initiated and/or created off-campus involving the inappropriate use of the Internet or web-based resources if such conduct poses a threat or substantially interferes with or disrupts the work and discipline of the schools, including discipline for student harassment and bullying.

Internet safety policy

For purposes of this policy, this is the district's "Internet safety policy." This policy includes provisions to address access by minors to inappropriate material on the Internet; the safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications; unauthorized access, including so-called "hacking" and other unlawful activities by minors online; unauthorized disclosure, use and dissemination of personal identification information regarding minors; and measures designed to restrict minors' access to materials harmful to minors. Prior to accessing the network, Internet or email services, students and staff will receive instructions on the appropriate use of these services. Students and staff must sign a form annually acknowledging that they have read and understand this policy, that they will comply with the guidelines set forth herein and that they understand the consequences for violating these guidelines.

Terms and conditions of use Acceptable Use

The purpose of the district's educational network is to support research and education in and among academic institutions by providing access to unique resources and the opportunity for collaborative work. All use of the Internet and network must be in support of education and research and be consistent with the educational goals of the district. Use of other networks or computing resources must comply with the rules governing those networks. Transmission of any material in violation of federal or state laws or regulations is prohibited. This includes, but is not limited to, the following:

- copyrighted material
- materials protected by intellectual property
- threatening or obscene material
- material protected by trade secret

Access to computer systems and networks owned or operated by the district imposes certain responsibilities and obligations on users and is subject to district policies and local, state and federal laws. Students may

access the Internet for educational or work-related purposes at any time that is not disruptive and does not interfere with the performance of other responsibilities.

Staff members who are exploring the websites with a class do not need special parental permission for students for such activity if the teacher is in control of the navigation to known educational sites. All computer and Internet usage by students is to be consistent with the Cherokee County School District mission and policies.

Permitted uses of Internet and email

- Users will utilize the system for educational and professional development activities only.
- Users may download text and other approved files attached to email messages or from the Internet for school-related business only. Large files should be downloaded during off-peak hours whenever possible.

Procedures for use

- Users will subscribe only to high-quality discussion group mail lists that are relevant to their educational or professional/career development.
- Users will not post chain letters or engage in spamming. Spamming is sending an unnecessary message to a large number of people.
- Users will not use their email account for personal use, with the exception of contacting a family member or emergency, work or school-related purposes.
- Users are not allowed to access personal email accounts through district Internet connections.
- Users should not utilize the district email system to advertise or solicit business.
- Users should adhere to common rules for email etiquette.

Email retention

The district intends to set a district-wide guideline regarding the scope and duration of email retention. The information includes, but is not limited to, messages, communication headers, recipients and senders, and files and attachments that are either stored or shared via electronic mail. Questions about these guidelines should be addressed to the office of technology. This email retention policy applies to all district employees, regardless of job or department. This policy is to be observed in both conjunction with the district's acceptable use for network, internet and email services and the district's adherence to the Freedom of Information Act. Any email - regardless of sender, recipient, content, message attachment or intended audience - is considered subject to this policy. The duration of email storage will be set at five years. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

General prohibitions

- Users may not use the district system for commercial purposes, defined as offering or providing goods or services or purchasing goods or services for personal use. This prohibition does not include use of the district's sales and promotions area. The district will not be responsible for any obligations resulting from any unauthorized use of the system or use of the sales and promotions area.
- Users may not use the system for political activities.

Personal safety

- Students will not post personal contact information about themselves or other people unless it is in conjunction with a specific teacher-approved assignment or approved college/career communication.
- Personal contact information includes address, telephone number, school address, social security numbers, etc.
- Students will not agree to meet with someone they have met online without their parent/legal guardian's approval.
- Students will promptly disclose to an administrator, teacher or other school employee any message they receive that is inappropriate or makes them feel uncomfortable.

Illegal activities

- Users will not attempt to gain unauthorized access to the email system, the district web pages, or any other computer systems through district email, network access and/or Internet. Users will not attempt to perform functions that exceed their authorized access. This includes attempting to log in through another person's account or access another person's files.
- Users will not make deliberate attempts to disrupt the computer system performance or destroy data by spreading computer viruses, malware or by any other means.
- Users will not use the district system to engage in any other illegal act, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of another person or any other activity that violates existing district policies. Reference to such activities will not even be made in a joking manner or as a prank.
- The district will contact law enforcement, consistent with state law, when criminal conduct occurs, as set forth in S.C. Code Section 59-24-60.

System security

- Users will not share their account information (user ID and/or password) or attempt to log in to another user's account. Any sharing of user ID or password will result in immediate restriction or removal of account privileges. The only potential exception is the sharing of information with IT staff if requested for troubleshooting purposes.
- Users will immediately notify the IT staff if they have identified a possible security problem (students should notify a teacher and/or principal). Do not actively seek security problems but immediately report any potential issues that are found.
- Users will not download or install any unauthorized software or install any unauthorized hardware, e.g., computers, wireless access devices, printers or any network equipment, etc.
- Users will not knowingly execute any files containing viruses, other files with illegal content or in any other way knowingly spread computer viruses.

Bullying/Cyberbullying

The district will educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response. The superintendent or his/her designee will develop a program to educate students on these issues.

Cyberbullying is an intentional electronic act or series of acts directed at another student or students that creates substantial interference with a student's education, creates a threatening environment or disrupts the orderly operation of school. These acts include, but are not limited to, the following:

- sending hurtful, rude or mean text messages, images or videos

- spreading hurtful messages, rumors or lies about others by email or on social networks
- creating websites, videos or social media profiles that embarrass, humiliate or make fun of others

Cyberbullying is strictly prohibited by the district and will result in disciplinary action. Any student who witnesses or has reliable information that a student has been subject to harassment, intimidation or bullying (including cyberbullying) should report the incident to the principal or the designated school contact person. Reports may be anonymous; however, formal disciplinary action will not be taken solely on the basis of an anonymous report.

Use of appropriate language

Restrictions against inappropriate language apply to public messages, private messages and material posted on web pages.

- Users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful or gang-related language or symbols.
- Users will not post information that could cause damage or a danger of disruption of network services. Users will not engage in personal attacks, including, but not limited to, prejudicial or discriminatory remarks.
- Users will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a user is told by a person to stop sending messages, he/she must stop.
- Users will not use any language that threatens another person, whether it is the recipient of the message or a third party.
- Users will not knowingly or recklessly post false or defamatory information about a person or organization.

Access to inappropriate material

Users will not use the district system to access material that is profane or obscene, e.g., pornography, that advocates illegal acts, or that advocates violence or discrimination towards other people, e.g., hate literature. Adult users who mistakenly access inappropriate information or images should immediately report this to the district help desk or to the district technology director. This action will initiate the process to have the materials blocked. Students who mistakenly access inappropriate information or images should immediately report this to the attending teacher. The school principal should be notified if it is deemed warranted. This will protect users against an allegation that they have intentionally violated the acceptable use for network, internet and email services. Students are expected to follow parental guidance regarding limitation of access to additional types of inappropriate materials.

Respect for privacy

Users will not post private information about another person. The district reserves the rights to examine, restrict or remove any material that is on or passes through its network, just as it does any other work or material generated or brought to school by staff and students. Access to electronic information related to any student or staff member will be governed by the same policies that would apply to that information if it were not in electronic format.

Penalties for improper use

Any employee who violates the terms of this policy or otherwise misuses email or the Internet and/or technology to access inappropriate material will be subject to disciplinary action, up to and including dismissal. In addition, the privilege of accessing the Internet and email services will be subject to

cancellation. Students who violate the terms of this policy or who otherwise misuse their access to email or the Internet also will be subject to disciplinary action in accordance with the district's student behavior code, JICDA-R. Internet and email privileges may also be cancelled. Violations of the laws of the United States or the State of South Carolina also may subject the user to criminal prosecution. If the user incurs unauthorized costs, the user, as well as the user's parent/legal guardian if the user is a student, will be responsible for all such costs. Any user who deliberately damages district hardware will be charged for any repair or replacement costs. Cost to repair damages that result from deliberate attempts to override or disable protection software will be charged to the user.

Warranty

The district makes no warranties of any kind, whether expressed or implied, for the service it is providing. The district will not be responsible for any damages suffered by any user. This includes loss of data resulting from delays, non-deliveries, misdirected deliveries or service interruptions caused by the system's negligence, user errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The district specifically denies any responsibility for the accuracy or quality of information obtained through its services. Materials on web pages reflect an individual's thoughts, interests and activities, such web pages do not, in any way, represent individual schools or the district, nor are they endorsed or sanctioned by any individual school or the district. Concern about the content of any page(s) created by students or staff should be directed to the building principal of that school. Given the rapid change in technology, some of the technical standards outlined in this policy may change throughout the year. The district's director of technology, with approval of the district superintendent, will make such changes. This policy may be updated on an annual basis or more frequently if required.

School board policies

All documents on the district's server(s) must conform to board policies and regulations, as well as established district guidelines. Copies of board policies are available in all school offices and on the district website. Persons developing or maintaining web documents are responsible for complying with these and other policies, regulations and guidelines. Some of the relevant issues and related board policies include the following:

- Electronic transmission of materials is a form of copying. As specified in district policy, no unlawful copies of copyrighted materials may be knowingly produced or transmitted via the district's equipment, including its web server(s).
- Documents created for the web and linked to district web pages must meet the criteria for use as an instructional resource in accordance with district policies, regulations and guidelines.
- Any links on district/school web pages that are not specifically curriculum related must meet the criteria established in the district's technology acceptable use for network, internet and email services. Any other non-curricular materials should be limited to information about other youth activities, agencies or organizations which are known to be non-sectarian, exclusively devoted to community interests or child welfare, non-profit and non-discriminatory. Web page links may not include entities whose primary purpose is commercial or political advertising.
- All communications via the district web pages will comply with the district's technology acceptable use for network, internet and email services and the district's student behavior code policy. Offensive behavior that is explicitly prohibited by these policies includes religious, racial and sexual harassment

and/or violence. Any student information communicated via district web pages will comply with district policies on data privacy and public use of school records.

Adopted 3/11/97; Revised 12/10/12, 6/10/13

Legal references:

Federal law:

47 USC Section 254(h) - Children's Internet Protection Act.

The Digital Millennium Copyright Act of 1998, Section 512 - Limitations on liability relating to material online.

S.C. Code of Laws, 1976, as amended:

Section 10-1-205 - Computers in public libraries; regulation of Internet access.

Section 16-3-850 - Encountering child pornography while processing film or working on a computer. Section 16-15-305 - Disseminating, procuring or promoting obscenity unlawful; definitions; penalties; obscene material designated contraband.

Section 59-19-90 - General powers and duties of school trustees.

Court cases:

APPENDIX D: Cherokee County School District Cherokee County School District Mobile Computing Device Discipline Plan

APPENDIX D: Cherokee County School District Cherokee County School District Mobile Computing Device Discipline Plan

Level 1 Classroom Violations

Include but are not limited to: Bringing district issued device uncharged to class, being unprepared for class (no District Issued device), careless, irresponsible use, or off-task behaviors. Sharing classwork, homework, tests, or other material determined to be individual work done by an individual-not a group

All Level 1 Violations should be handled by the Classroom Teacher in the following manner:

1st Offense- Teacher-based discipline

2nd Offense- Teacher-based discipline

3rd Offense- Teacher-based discipline with parent contact (A call or email contact must be attempted in one or more methods and administration notified if contact cannot be made) 4th Offense Referral to Administration

Examples of teacher-based discipline include:

- Verbal redirection
- Student/teacher conference
- Restricted use in the classroom
- Alternate assignments - Such as Paper and pencil assignments
- Teacher-Assigned Detention
- Parent/Teacher Communication and/or Conference

**And/or Administrative Override

Level 2 Violations or Examples of Minor Misuse of the District Issued Device

- Use during unauthorized times or locations
- Unauthorized use of Internet or computer games-Playing Games
- Giving out personal information, for ANY reason
- Other misuse as determined by the administration
- Disruptive email(s) from student to student; conversations as opposed to work related to school

Level 2 Violations or Minor Misuse of District Issued Device will result in restricted use and/or temporary forfeiture as follows:

1st Offense- Mandatory parent conference at the school AND WARNING about continuing offenses and consequences

****A parent letter describing the next steps for Level 2 Violations will be signed at this conference.**

It describes for the parent and student what will happen on the next violation(s) including consequences.

2nd Offense- Two days of ISS and Individuals will be allowed to use their computers in ISS

3rd Offense- 2 days of OSS and The computer will be confiscated for the 2 days of suspension.

4th Offense- 3 days of OSS and The computer will be confiscated for the 3 days of suspension.

Subsequent Offenses will result in Alternative School Placement and/or a

Recommendation for Expulsion.

A police report will be filed if the device violation includes explicit or inappropriate content is

Criminal or illegal in nature.

****And/or Administrative Override**

Level 3 Violations or Examples of Major Misuse of District Issued Device

Students should never login into Google Chrome or download any extensions or add on. Doing so will be a violation and may cause other inappropriate material to be downloaded to your device.

- Sharing username and/or password or other personal school district account information
- Use of ANY messaging system not approved by the District Technology Department and/or school.
- Downloading and/or Using websites to obtain purchased or illegal term papers, book reports, or other forms of required student work
- Unauthorized downloading, installing, transmitting music, games, copyrighted material and/or other applications
- Deleting district system applications and changing personal mobile computing device settings, (exceptions include personal settings such as font size, brightness of screen, etc.....)

1st Offense - 3 days OSS and Computer will be confiscated for the 3 days of suspension.

Parent conference with student and parent.

2nd Offense 5 days OSS- Computer will be confiscated for the 5 days of suspension.

Parent notification of violation and discipline.

3rd Offense 10 days of OSS and confiscation of computer pending the discipline decision; and possible recommendation for expulsion and/or Alternative School Placement; Law Enforcement will be notified as needed

****Note:** The Administration reserves the right to handle any of the above actions or any other action determined to be a Misuse of Technology in the manner they think is most appropriate for all concerned.

A police report will be filed if the device violation includes explicit or inappropriate content that is Criminal or illegal in nature. **And/or Administrative Override

Level 4- Violations or Examples of Extreme Major Misuse of District Issued Device

- Bypassing the Cherokee County School District Website/Web filters
- Actions violating board policy or public law including Bullying, Cyber-Bullying, harassment, intimidation, etc.....
- Sending, transmitting, accessing, uploading, downloading, photographing/filming others without permission of the district and/or school and/or against their will, or disrupting obscene, offensive, profane, threatening, pornographic, obscene sexually explicit materials with the intention to demean or harass others
- VPN downloading and/or proxy use for internet access, (other things from IT); hacking district systems; batch files or scripts for malicious intent
- Gaining access to other students, staff, or school district employee's accounts, files, and/or data
- Vandalism (any malicious attempt to harm or destroy the personal mobile computing device); Restitution Required
- Inappropriate searches will deliver a report to the CCSD Technology Department; searching for inappropriate content/material will lead to appropriate discipline

Level 4 Consequences

1st Offense 5 days OSS; Computer will be confiscated for the 5 days of suspension.

Mandatory Parent Conference

2nd Offense 10 Days of OSS, Computer will be confiscated for 10 days of suspension;

Mandatory Parent Conference;

**3rd Offense Alternative School Placement and/or Recommendation for Expulsion
Appropriate law enforcement notification and/or charges**

****Note:** The Administration reserves the right to handle any of the above actions or any other action determined to be a Misuse of Technology in the manner they think is most appropriate for all concerned.

A police report will be filed if the device violation includes explicit or inappropriate content of a student that is Criminal or illegal in nature.

****And/or Administrative Override**

Possession and use of personal and/or district issued electronic devices on school property acknowledges consent to search the contents of the device in a school or criminal investigation. In such investigations, students will provide necessary login information as needed. Misuse of technology outside school that impacts the people or environment on campus may also necessitate similar disciplinary consequences and searches.

**The Cherokee County District Laptop Handbook will describe the costs involved in restitution of any damage to the District Issued Laptop.

**Note: The administration reserves the right to handle any of the above actions or any other action determined to be a Misuse of Technology in the manner they think is the most appropriate for all concerned.

**And/or Administrative Override

Any malicious damage to a District Issued Device must be reported to school and/or police within 48 hours of the occurrence. Failure to report to the school and/or police will result in that the student the District Issued Device belongs to being solely responsible. Students who damage another student's computer will be held accountable after an investigation is completed from the report given to the school and/or police.

APPENDIX E: Cherokee County School District Mobile Device Discipline Plan for Primary and Elementary Students

CCSD-Primary and Elementary School Technology Mobile Device Discipline

Minor misuse will result in restricted use and/or temporary forfeiture of the device as follows:

1st Offense = Mandatory parent conference

Recess Detention, lunch detention and other suitable and appropriate behavioral interventions may be used after the Parent/Student Conference

2nd Offense = Mandatory Parent conference

Recess Detention, lunch detention and other suitable and appropriate behavioral interventions may be used after the Parent/Student Conference

3rd Offense = **Treated as a Major Misuse** (see Major Misuse of Mobile Device listed below)

Minor misuse will result in restricted use and/or temporary forfeiture of the device as follows:

1st Offense = Mandatory parent conference

Recess Detention, lunch detention and other suitable and appropriate behavioral interventions may be used after the Parent/Student Conference

2nd Offense-Parent conference

Student must check the device in/out from the classroom teacher for 5 school days

3rd Offense-Parent conference

Student must check the device in/out from the classroom teacher for 10 school days

4th Offense = Application of the following consequences as needed:

In-School Suspension (ISS)

Out-of-School Suspension (OSS)

Examples of Major Misuse of Mobile Device

- Bypassing the Cherokee County School District Web filter
- Actions violating board policy or public law; law enforcement will be notified when necessary
- Deleting district system applications and changing of personal mobile computing device settings (exceptions include personal settings such as font size, brightness, etc.)
- Sending, transmitting, accessing, uploading, downloading, or distributing obscene, offensive, profane, threatening, pornographic, obscene or sexually explicit materials
- Use of chat rooms or sites selling term papers, book reports and other forms of student work
- Spamming (disruptive email, messages including iMessages)
- Gaining access to another student's accounts, files and/or data
- Use of the school's Internet or e-mail accounts for any illegal activity
- Vandalism (any malicious attempt to harm or destroy the personal mobile computing device)
- Transmission or access of obscene, offensive or threatening materials or materials intended to harass or demean

Major Misuse will be handled as follows:

1st Offense = 2 - 5 days OSS, mandatory parent conference, and temporary forfeiture

2nd Offense = 10 days OSS, district-level hearing, and forfeiture as warranted

3rd Offense = Alternative School placement and/or expulsion; appropriate law enforcement charges

Note: The administration reserves the right to handle any of the above actions or any other action determined to be a misuse of technology in the manner they think is the most appropriate for all concerned.

Parent Signature: _____

Date: _____

Student Signature: _____