

Purpose

The Cherokee County Board of Education ("CCBOE") provides all students with access to technology resources for educational purposes. Students are expected to follow the rules set forth in this responsible use policy, the Cherokee County Board of Education Student Handbook ("student handbook") and the law in the use of the technology resources available.

Definitions

The term "technology" in this document, is intended as a broad interpretation referring to, but not limited to computers, hardware, software, network devices, peripherals, the Internet, e-mail, websites, online class management systems and other online environments.

The term "network" refers to the collection of electronic devices including, but not limited to, computers, printers, scanners, cameras, copiers, connectivity, and other electronic and connectivity devices that may or may not have access to the Internet, networked resources, electronic mail and other devices available through the local network and the Network.

Student Access and Permission

All students will have access to the Internet and other technology resources through their classroom, library, or other school computers. This includes access to, but is not limited to, online curriculum, web-hosted software, email, textbook resources and assessments. The District has the right to place restrictions on the material accessed or posted through the system. Access to the CCBOE Computer Network ("network") may be revoked as stated in the student handbook. In addition, the policies, rules, and regulations also apply to personally-owned technology resources brought on to school property.

The Internet will be filtered as required by the Children's Internet Protection Act (CIPA) and student activity on the network will be monitored for student safety and responsible use.

Students should only use technology resources under the direct supervision of their teacher. In addition, students will need the specific permission of their teacher in order to publish information to the district, school, or class webpages, blogs, wikis, or other social media sites. When doing so, students are expected to adhere to applicable design requirements, online safety practices, and general rules of good conduct. Specific permission is also required in order to take technology resources off school grounds. A permission form, including specific instructions and conditions, will need to be signed.

Search and Seizure

There is no expectation of privacy in the contents of personal files and use on the CCBOE system. Routine maintenance and monitoring of the network may lead to discovery that students have violated this policy, the student code of conduct, or the law. An individual search will be conducted if there is suspicion that a student has violated this policy or the law.

Due Process

The District will cooperate fully with local, state, or federal officials in any investigation related to any illegal activities conducted through the network. In the event there is a claim that a student has violated this policy or the code of conduct in the use of the network, the due process policy as outlined in the code of conduct will be followed. Additional restrictions may be placed on the use of the Internet and/or computers and/or other resources of the network as a disciplinary measure.

Limitation of Liability

The District makes no guarantee that the functions or the services provided by or through the District system will be error-free, without defect, or always available. The District will not be responsible for any damage students may suffer, including but not limited to, loss of data or interruptions of service. The District is not responsible for the accuracy or quality of the information obtained through or stored on the system. The District will not be responsible for financial obligations arising through the unauthorized use of the system.

Adoption of Procedures and Guidelines

Management of technology resources will be directly related to the procedures developed by the Superintendent and the Technology Office. The Superintendent and the Technology Coordinator are authorized to develop additional rules and procedures regarding the daily use and management of technology resources to ensure proper use through such documentation as the "Technology Standard Operational Procedures" document. This document will be available on the district website for review.

Unacceptable Uses of Technology**Personal Safety:**

- Students will not post or expose personal private information about themselves or others such as social security number, birthday, pin number, password, etc.
- Students will not agree to meet with someone they have met online.
- Students will promptly disclose to their teacher or other school district employee any message and/or material received and/or see that is inappropriate or makes them feel uncomfortable.

Illegal Activities:

- Students will not attempt to gain unauthorized access to the network or to any other computer system through the network or go beyond their authorized access. This includes attempting to log in through another person's account or access another person's files.
- Students will not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means.
- Students will not use technology resources 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 a person, etc.

System Security:

- Students are responsible for their individual actions while accessing the network and should take all reasonable precautions to prevent abuse and misuse of the system for activities other than of an educational nature.
- Students will immediately notify the District Technology Coordinator if a security problem has been discovered. Students are not authorized to "look for" or "test" security problems. This action may be construed as an illegal attempt to gain access.
- Students will avoid the spreading of computer viruses through e-mail or the downloading of files from the Internet by following the guidelines established for these activities established by the Technology Office.
- Students will not develop or install malicious software (on or off campus) designed to infiltrate computers, damage hardware or software, spy on others, or compromise security measures.
- If students have an account of any type that is issued through the District, students will not share password or account information with anyone and will protect their account from unauthorized use.
- Students will not attempt to circumvent, bypass, disable, exploit, workaround, break, or render ineffective in any manner whatsoever the security, protection, and/or filtering measures of the network. Any such attempt, whether successful or not, will result in disciplinary action as outlined in the student code of conduct.

Inappropriate Language:

- Students will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language. Students will not post information that could cause damage or a danger of disruption to network use and/or services and/or access.
- Restrictions against inappropriate language apply to public messages, private messages, and material posted on Web pages.

Harassment:

- Students will not bully or harass another person as defined by the anti-harassment policy in the student handbook. Online harassment, otherwise known as "**cyberbullying**," is acting in a manner that distresses or annoys another person.
- Students will not engage in personal attacks, including prejudicial or discriminatory attacks.
- Students will not knowingly or recklessly post false or defamatory information about a person or organization.

Inappropriate Access to Material

- Students will not use the network to access material that is profane or obscene (pornography), that advocates illegal acts, that advocates violence or discrimination towards other people (hate literature), is illegal, or has no educational value.
- If inappropriate information is mistakenly accessed, students should immediately notify their teacher or other school official of the time and nature of the site accessed. This will protect students against a claim that they have intentionally violated this policy.
- Parents should instruct their child if there is additional material that they think would be inappropriate to access. The district fully expects that students will follow their parent's instructions concerning this matter.
- Students will not use the network for purposes that are personal in nature and are not related to their education and/or specific school assignments.

Respect for Privacy:

- Students will not attempt to read, delete, copy, forward, or modify e-mail or electronic files of others.
- Students will not repost a message that was sent privately without permission of the person who sent the message.
- Students will not post private information about another person.
- Students will not send and/or access electronic information anonymously.
- Students will not falsely pose as an employee of the Board of Education on any website, online forum, social networking site, or other online venue.
- Students will not post an image or the intellectual property of others without their permission.

Respecting Resource Limits

- Students will use the system only for educational purposes.
- Students will not download any file unless under the direct supervision of a teacher.
- Students will not store unauthorized material on computers and/or the network. Students will only store materials authorized by their classroom teacher. Students will remove materials promptly to ensure storage space is not over utilized and/or abused. There is no guarantee of the availability of storage and/or the ability to save and/or retrieve information.
- Students will not mishandle the equipment of the network and will take reasonable precautions to safeguard it from abuse and misuse.
- Students will not attempt to install, copy, delete, setup, remove, monitor or modify in any way software from any computer or system on the network without permission from the Technology Office.
- Students will not attempt to use or gain access to software that is not specifically allowed for educational purposes. Students will report such software discovered to their teacher immediately and provide information on where the software is located.
- Students will not post chain letters or engage in "spamming". Spamming is sending an annoying or unnecessary message to a large number of people.
- Individual subscriptions to mailing lists, news groups, forums, chat rooms, and other similar discussion type forums are not authorized for students.

Plagiarism and Copyright Infringement

- Students will not plagiarize works including written, graphical, or pictorial data that is found on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to you.
- Students will respect the rights of copyright owners. Copyright infringement occurs when someone inappropriately reproduces a work that is protected by a copyright. If a work contains language (such as Creative Commons licensing – some rights reserved or is protected by copyright – all rights reserved) that specifies appropriate use of that work, the expressed requirements should be followed. If students are unsure whether or not they can use a work, students should request permission from the copyright owner.

Parental Request for Restricted Access

If you or your parent and/or guardian do not wish for you to have access to the Internet, email and/or network access, your parent and/or guardian **must notify your school principal in writing**. This will not prevent students from viewing Internet sites or other technology resources presented by school personnel or by other students as part of a lesson, or from using web-hosted software applications used by the school such as, but not limited to, CompassLearning Odyssey, Renaissance Place (AR, STAR), online textbook resources and assessments. In the event of written notification requesting access restrictions by a parent and/or guardian, school personnel will take appropriate steps to restrict the student from using technology resources independently. Teachers will provide alternate non-technology based assignments on the same content.

Acknowledgement/Agreement Form

The Cherokee County Board of Education has established the Student Technology Responsible Use Policy for the safety and protection of all students. Violations of this policy statement are subject to the Cherokee County Board of Education code of conduct.

By signing the Student Handbook Acknowledgement Form, students and parents affirm that they understand and agree to follow the rules and guidelines set forth in the Student Technology Responsible Use Policy. However, failure to sign or return a signed form does not release students from their obligation to abide by these rules and regulations in the Student Technology Responsible Use Policy and all other applicable Board policies.