Student/Parent Chromebook Handbook

Section 1:

Student's First Name _____

Student's Last Name _____

Student's Grade Level _____

Student's School _____

Section 2:

Tutorial video: *http://youtube.com/watch?v=RIL4Qn4XgU4*

Watched Video _____ *(please initial)*

Section 3:

Why Digital Learning?

Digital access to content and continuous communication is central to how we learn and work today. Accessing information in a digital format allows for students to work in real time, using multiple media formats. Plus, this allows for a much higher level of collaboration among teachers and students, as well as among students themselves as they work together on projects.

In a digital environment, students have a more robust way of learning at any time in any location through which there is access. With that said, accessing content digitally will not eliminate hard copy text which will be used when appropriate.

Why Take Devices Home?

If we are truly going to provide students with access to their education 24/7 using digital content, then they must have the tools to do so. While we know that some families may not have access to the Internet at home, students will be able to access their Google Drive files via their device—even without Internet at home. In addition, we are partnering with business and other agencies to provide students access to the Internet after school hours. If we want to develop a community of learners, then we

need to create opportunities for students to access their education at any time and to trust them to effectively use the tools provided.

General Guidelines for Students

In this digital learning environment, there are expectations that will support innovative teaching and learning. Students are expected to:

1. Use Chromebooks to enhance their educational experience
2. Know and follow the CCSS Acceptable Use Policy and the CCSS Student Code of Conduct
3. Keep Chromebooks—which includes the device and accessories—in good condition, as they are the property of CCSS
    a. Remember to bring the Device and charging cord to school every day
    b. If applicable, keep the Device in its protective case at all times and carry it using the handle or shoulder strap
    c. When not in use, ensure Devices are stored in a secure location
    d. Log-off or lock Devices when not in use
    e. Fully charge the Device each night
    f. Do not leave the Device in a vehicle
    g. If ever in a situation when someone is threatening you for your Device, give it to them and tell a staff member as soon as you arrive at school
    h. Do not put personal markings, stickers, etc. on the surface of the Device
4. Use Chromebooks to support school district learning goals
5. Follow rules and guidelines at all times, whether on or off campus
6. Know that all activity, including emails and files, on CCSS equipment or the network are subject to review
7. Notify a staff member immediately if they come across information, images, or messages that are inappropriate, dangerous, threatening, or make them feel uncomfortable
8. Follow existing copyright laws and educational fair use policies
9. Keep their login information private
10. Understand how to use Google Apps for Education, including correctly storing files on their Google Drive account
11. Students will only be able to access the network using school issued devices.

Technology Discipline

List of Violations (not exhaustive)

- Email, instant messaging, internet surfing, computer games (off-task)
- Copying and pasting without citing sources (plagiarism)
- Cyber bullying
- Damaging or defacing Chromebook or accessories
- Using profanity, obscenity, racist, or discriminatory terms
- Accessing pornographic material
- Accessing inappropriate files or files dangerous to the integrity of the network
- Using a Chromebook account authorized to someone else
- Deleting browser history
- Using electronic resources for individual profit, for advertisements, or for political action
- Unauthorized downloading or installing software or other media
- Modifying district browser settings
- Attempting to bypass the district's Internet filter or profile restrictions (Proxy sites)

General Guidelines for Parents and Guardians

CCSS makes every effort to equip parents/guardians with the necessary tools and information to ensure effective use of Chromebooks to support instruction in the home. Parents are vital partners in the success of this initiative. We ask parents/guardians to:

1. Review General Guidelines for Students with their child(ren)
2. Monitor to ensure appropriate student use
3. Model the effective use of technology when applicable
4. Communicate with personnel when issues arise
5. View the Parent Orientation video for the Chromebook take-home
6. Use Parent Portal for student information
7. Access online student resources to support learning at home
8. Engage with their child(ren) and review work, including projects and other assignments
9. Sign the Student/Parent Chromebook Agreement
10. Be responsible for damaged, lost, or stolen Chromebook
11. Students will only be able to access the network using school issued devices.

Damaged, Lost, or Stolen Devices

Chromebooks issued to students will be recorded by serial number and asset tag number. Students are responsible for all Chromebooks issued to them. If a Chromebook is lost or damaged, the student will be required to pay for it as determined by the school administration.

Repairs

General wear and tear problems, including any software issues, will be covered by the district's Technology Support Services division at no charge. Temporary replacements, known as "loaners," are available at each school so that learning is not disrupted by the repair process. Students are responsible for the care of the loaner while issued to them. The same guidelines outlined above apply to loaners.

Lost/Stolen Equipment

In the event of lost equipment, a report must be made to school personnel. The district will make every effort to recover lost devices. Students will be provided with a loaner.

Chromebook Security

Software

Security is in place on the Chromebook to prevent activities including downloading or installing software on the Chromebooks, removing software, changing system settings, etc.

Internet Filtering

CCSS maintains an Internet filtering software package the extends to off-site as well. This program automatically filters all student access to the Internet when in school and at home or other Internet-enabled locations.

Identification

Chromebooks may be identified in the following ways: serial number, asset number, CCSS label with barcode, security sticker adhered to the back of the Chromebook, engraved CCSS logo on the outside of the Chromebook. Modifying or deleting such marks or labels violates district policy, as well as local and federal laws.

Read Guidelines _____ *(please initial)*

Section 4:

Coweta County School System
Internet Access – Students

Terms and Conditions for Use of the Internet /Internet Safety Policy

It is the policy of the Coweta County School System to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors, and (d) comply with the Children's Internet Protection Act [Pub. L No. 106-554 and 47 USC 254(h)].

Privileges - The use of Internet is a privilege, not a right, and inappropriate use will result in cancellation of those privileges.

> **Each student must participate in general information training concerning the appropriate educational use of the Internet before the student will be allowed access to the Internet. Students will not have access privileges from home. Students will have access privileges only at school under the supervision of a teacher. Parents or guardians may attend an informational meeting if they have questions or concerns.**

Unacceptable Usage

The user is responsible for all his/her actions and activities involving the network. Examples of prohibited conduct include but are not limited to the following:

1. Accessing materials or communications that are
   a. Damaging to another persons reputation
   b. Abusive
   c. Obscene
   d. Sexually oriented
   e. Threatening or demeaning to another person's gender or race
   f. Contrary to the school's policy on harassment
   g. Harassing
   h. Illegal.
2. Sending, creating, or posting materials or communications that are
   a. Damaging to another person's reputation
   b. Abusive
   c. Obscene
   d. Sexually oriented
   e. Threatening or demeaning to another person's gender or race
   f. Contrary to the school's policy on harassment
   g. Harassing
   h. Illegal
3. Using the school's computer hardware or network for illegal activity such as copying software or violation of copyright laws.
4. Making copies of software on any school's computer or computer system.
5. Copying or downloading copyrighted software for one's own personal use.
6. Using the network for private financial or commercial gain.
7. Loading or using games, public domain, shareware, or any other unauthorized programs on any of the school's computers or computer systems.
8. Purposely infecting any school computer or network with a virus or program designed to damage, alter, or destroy data.
9. Gaining unauthorized access to network resources.
10. Attempting to bypass Internet filtering devices.
11. Invading or attempting to use another person's user name or password.
12. Posting or plagiarizing work created by another person without their consent.
13. Posting anonymous messages.
14. Using the network for commercial or private advertising.

15. Forging electronic mail messages.
16. Attempting to read, alter, delete, or copy the electronic mail of other system users.
17. Using the school's computer hardware, network, or Internet link while access privileges are suspended.
18. Using the school's computer hardware, network, or Internet link in a manner that is inconsistent with a teacher's directions and generally accepted network etiquette.
19. Attempting to alter the configuration of a computer of any of the school's software. Examples include changing screen colors, backgrounds, screen savers, etc.
20. World Wide Web- Students do not have permission to create "home pages" or directories. Student work will be published only under the direction of the supervising teacher.
21. Acceptance of Terms and Conditions - All terms and conditions as stated in this document are applicable to Coweta County students. These terms and conditions reflect the entire agreement and understandings of the parties. These terms and conditions shall apply to the laws of the State of Georgia and the United States of America.
22. Every student of the Coweta County School System will be given a unique user name and password to logon onto the County's network. All users must use their own logon credentials to access the network. Giving this username and password to another individual is a direct violation of Coweta County Board policy.

Access to Inappropriate Material

To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet access to inappropriate information.

Specifically, as required by CIPA, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.

Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the Coweta County School System online computer network when using electronic mail and other forms of direct electronic communications.

Specifically, as required by CIPA, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking', and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Education, Supervision and Monitoring

It shall be the responsibility of all members of the Coweta County School System staff to educate, supervise, and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

Education for minors shall include: appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms; and cyber bullying awareness and response.

Cyber bullying

Cyber bullying is when a child is threatened, harassed, humiliated, or embarrassed by another child using digital technologies such as the Internet.
Some examples of cyber bullying are:

- Pretending to be someone else online to trick others
- Spreading lies and rumors about others
- Tricking people into revealing personal information
- Sending or forwarding mean text messages
- Posting pictures of people without their consent

You can prevent cyber bullying if you "take 5" before responding to something you encounter online. You can stop communication with cyber bullies; and you can also report cyber bullying to your teachers.
Some ways to stay cyber-safe are:

- Never post or share your personal information online (this includes your full name, address, telephone number, school name, parents' names or Social Security number).

- Never share your passwords with anyone, except your parents.
- Never meet anyone face to face whom you only know online.

Coweta County School System

Internet Access – Students

I understand and will abide by the Terms and Conditions for Internet. I further understand that any violation of the regulations is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, school disciplinary action may be taken and/or appropriate legal action may be initiated.

_____

Student Signature

_____

Student Name (Please Print)

_____ _____

Home Phone Date

_____ _____

Home address City/Zip Code:

_____ **Yes**, I give permission for my child to have Internet access.

_____ **No**, I do not give permission for my child to have Internet access.

_____ _____

Parent or Legal Guardian Signature Date

_____

School