Coffee County School System Technology Responsible Use and Internet Safety Policy (RUP)rev.2024 Board Approved 05-13-2024

The Coffee County School System (CCSS) provides students and staff with access to computers, network systems, and other technology equipment to support educators in delivering effective instruction. Teachers or approved CCSS representatives are responsible for providing educationally relevant lessons, supervision, and instruction to help students get the most benefit from available technology resources. Students and staff are responsible for using the systems for educational purposes, respecting other users, and complying with the Children's Internet Protection Act (CIPA) [Pub. L. No. 106-554 and 47 USC 254(h)] and Tennessee Department of Education requirements as stated in Tennessee Code Annotated 49-1-221. In general, students and staff are permitted to use technology resources for educational purposes with the permission and guidance of a supervising CCSS staff member or approved CCSS representative provided the guidelines and restrictions herein set forth are followed.

The board intends that students and staff benefit from these resources while remaining within the bounds of safe, legal, and responsible use. Accordingly, the district establishes this policy to govern student and staff use of school district technological resources. This policy applies regardless of whether such use occurs on or off school district property, and it applies to all school district technological resources, including but not limited to computer networks and connections, the resources, tools and learning environments made available by or on the networks, and all devices that connect to those networks.

All students and staff must be informed annually of the requirements of this policy and the methods by which they may obtain a copy of this policy. Before using school district technological resources, students, student's legal guardians and staff must sign a statement or consent by digital acknowledgement indicating that they understand and will strictly comply with these requirements.

Consequences
Violations of this policy may result in disciplinary action up to and including revocation of user privileges, suspension, expulsion, termination (staff) and when applicable the involvement of appropriate law enforcement.

TECHNOLOGY RESOURCES
Technology equipment provided by the schools is the property of CCSS and is intended to be used by staff and students for educational purposes consistent with the goals of the school district. The use of school district technological resources, including access to the Internet, is a privilege, not a right. To maintain efficient functionality of the equipment and to ensure its appropriate use, the district reserves the right to monitor all network traffic, search all files stored on district-owned systems and to take such action as necessary to assure that system resources are available for their intended purposes. Therefore, users of district technology should have no expectation of privacy when using school networks or technology equipment. Additionally, users may not store personal files or data, install or remove software, modify system settings, perform maintenance or upgrades or otherwise alter existing systems without the express approval of a supervising CCSS Technology or approved CCSS representative. Users may not intentionally or negligently damage computers, computer systems, electronic devices, software, computer networks or data of any user connected to school district technological resources. Users may not knowingly or negligently transmit computer viruses or self-replicating messages or deliberately try to degrade or disrupt system performance. Users must scan any downloaded files for viruses. Users enrolled in classes that teach game design or theory may follow the curriculum of their respective courses to create games. Users enrolled in computer classes teaching network design or maintenance may, with the assistance of their instructor, create programs as required by the course curriculum.
Users are prohibited from engaging in unauthorized or unlawful activities, such as "hacking". Using the computer network to gain or attempt to gain unauthorized or unlawful access to other computers, computer systems or accounts will be subject to disciplinary action. Those who use district owned and maintained technologies to access the Internet at home are responsible for both the cost and configuration of such use.
Employees and students who are issued district owned and maintained equipment must follow these guidelines.

- Keep the equipment secure and in good working order.
- Use a protective case at all times. If not using a case, make sure that it is protected during transit.
- Do not remove, cover, obscure, or deface any portion of the District asset tag nor any other labels placed on the device by district personnel.

- Do not loan out the equipment, charger, or cords.
- Do not leave the equipment in your vehicle
- Do not leave the equipment unattended.
- Do not eat or drink while using the equipment or have food or drinks in close proximity to the equipment.
- Do not allow pets near the equipment.
- Do not place the equipment on the floor or on a sitting area such as a chair or couch.
- Do not leave the equipment near table or desk edges.
- Do not stack objects on top of the equipment.
- Do not leave the equipment outside.
- Do not use the equipment near water such as a pool.
- It is up to the user to back up data and other important files regularly. CCSS will at times perform maintenance on the equipment by imaging. All files not backed up to server/cloud storage space or other storage devices will be deleted during this process.
- Do not check the equipment as luggage at the airport. It is usually advisable to carry any district owned equipment on board with you rather than checking it as luggage.

NETWORK SYSTEMS

School computer systems exist in a networked environment that is designed with safeguards to ensure its dependability but which also relies on the goodwill of its users. Users who disrupt or compromise system resources by altering the network infrastructure or settings, attempting to acquire or use the login credentials of other users, introducing resource-draining applications, monitoring the network traffic of other users, bypassing existing security restrictions or filtering measures by any means including such items as proxies or VPNs, or otherwise compromise the integrity of the network will be subject to disciplinary action. This includes use of personal devices on the network.

INTERNET ACCESS

CCSS provides filtered internet access for educational and administrative purposes. In providing this access, CCSS attempts to limit the availability of web content that is inappropriate for students in the school environment. While these restrictions are typically sufficient to protect the innocent, it is impossible to completely prevent students from accessing inappropriate material and impossible to predict with certainty what information on the Internet students may access or obtain. Therefore, all students are responsible for using the Internet in an appropriate manner and are permitted access only through the school's filtered Internet service. Anyone who attempts to circumvent the filter system by either software or use of websites, access inappropriate Internet services or publish inappropriate content, or assist others in accessing or publishing such content or services are subject to disciplinary action and, when applicable, the involvement of appropriate law enforcement. The district is not responsible for content accessed by users who connect to the Internet via their personal mobile telephone technology services (e.g., 4G, 5G service).

Teachers shall make reasonable efforts to supervise students' use of the Internet during instructional time to ensure that such use is appropriate for the student's age and the circumstances and purpose of the use.

Inappropriate uses of the CCSS network include, but are not limited to:

- Pornography
- Gambling
- Storing, sharing, streaming or possession of copyrighted material
- Use of network for commercial purposes (Buying and selling for personal gain)
- Harassment, insulting, defaming or attacking others (Cyber Bullying)
- Illegal Activities
- Users of technological resources may not send electronic communications fraudulently (i.e., by misrepresenting the identity of the sender).
- Hacking or obtaining access to unauthorized systems
- Obscene Language
- Trespassing in other's files or folders
- Using another person's identity or password to access the network
- Damaging or modifying computer systems without permission from CCSS Tech Department
- Use of VPNs, Proxies, or other Remote Access Programs (including personal devices)

- Plagiarism of Internet resources

No user of technological resources, including a person sending or receiving electronic communications, may engage in creating, intentionally viewing, accessing, downloading, storing, printing, or transmitting images, graphics (including still or moving pictures), sound files, text files, documents, messages, or other material that is obscene, defamatory, profane, pornographic, harassing, abusive or considered to be harmful to minors. Users should be aware that possession/transmission of nude, or partially nude, images of a minor constitutes possession/transmission of child pornography. Should such activity be discovered by district personnel, the district must notify law enforcement personnel. All users must comply with policy 5.500 – Discrimination/Harassment of Employees (sexual, Racial, Ethnic, Religious) and 6.304 Student Discrimination/Harassment and Bullying/Intimidation when using school district technology.

Even though CCSS blocks certain sites, the faculty and staff are expected to diligently monitor students' computer and Internet usage. CCSS runs filtering software as required by CIPA(Childhood Internet Protection Act) and TN Senate Bill No. 3702 (49-1-221). CCSS provides robust digital resources for classroom instruction that have been found to meet the Federal Trade Commissions' (FTC) regulations in regard to the Child Online Privacy Protection Act (COPPA).

In accordance with the Board's goals and visions for technology, students may require accounts in third party systems for school related projects designed to assist students in mastering effective and proper online communications or to meet other educational goals. Parental permission will be obtained when necessary (i.e., when parental consent is needed by a site to meet CIPA or COPPA requirements) to create and manage such third-party accounts. Parents will provide this by signing or electronic acknowledgement of the CCSS Digital Learning Content Parental Consent Form included in this document. Teachers will reference the CCSS Approved Digital Resource List or receive approval from Technology when using any resource that requires Protected Personal Information (PPI) student data and to make sure that it is COPPA compliant.

Some of these resources may require student login credentials. At no time should a student log in and use an account other than the one that has been assigned for any particular service. The District technology staff has the right to remove any unauthorized or unlicensed software or media content, restrict the use/listening /watching of streaming media to preserve District bandwidth or to adhere to copyright laws. The district may restrict the use of games for students and staff with the exception of educational software that have been approved by the district.

The Board recognizes that parents of minors are responsible for setting and conveying the standards their children should follow when using media and information sources. Accordingly, before a student may independently access the Internet, the student's guardian must be made aware of the possibility that the student could obtain access to inappropriate material while engaged in independent use of the Internet. The parent and student must consent to the student's independent access to the Internet and to monitoring of the student's Internet activity and e-mail communication by school personnel. Parents will provide consent by signing or electronic acknowledgement of this RUP with the form provided at the end of this RUP.

Parents have the right to request a review of web resources used within the school to ensure they meet accessibility standards and align with inclusive practices. Requests for review for any reason should be submitted in writing to the student's school administration, specifying the particular web resource in question. The school will respond to parental requests for review within a reasonable timeframe and provide feedback on the steps taken or to be taken to address any identified accessibility issues.

EMAIL AND DOCUMENT ACCOUNTS

CCSS has partnered with Google to provide email,online accounts and digital services. This service is in full compliance with the provisions of The Children's Online Privacy Protection Act (COPPA). COPPA applies to PPI about a child that is collected online, such as full name, home address, email address, telephone number or any other information that would allow someone to identify or contact the child. No personally identifiable information is revealed to users outside Coffee County Schools. Student usage and disclosure of PPI is covered in other sections of this document.

Users shall not use passwords or user IDs for any data system for an unauthorized or improper purpose. All users, other than members of the Instructional Technology team, are prohibited from using another individual's ID or password. Email accounts will be issued to staff and appropriate students. Email accounts should be protected with strong passwords. Email accounts should not be shared with others. All emails are archived per CCSS policy. Anyone sharing his or her accounts or using anyone's account without permission of the Director of Schools or the Director of Technology may be subject to disciplinary action up to and including suspension, expulsion, termination (staff) and, when applicable, the involvement of appropriate law enforcement. Students and staff will NOT use a k12coffee.net account to sign into personal accounts (banking or gaming sites for instance) or any other service that is not for the explicit use for Coffee County Schools and such service is approved by the district technology. In other words, do not use "Sign In With Google"for any personal site or a service unless it is educational and approved by the district.
Student emails are filtered by the district and only allow communication with the k12coffee.net domain accounts with the exception of an allowed list of addresses. District personnel are able to see all messages sent to or from any student account, but will not examine messages unless directed to by a competent authority (Principal, Director of Schools, or Law Enforcement with proper documentation). Staff emails can be accessed only by request of the Director of Schools. Any abuse of the service (bullying, profanity and other violations stated by this RUP) may result in access of the service removed and users may be subject to disciplinary action. Under no circumstances should teachers or staff email a student using ANY account (for either party) other than those provided by the district. Specifically, teachers/staff should never email a student's personal email account and a teacher/staff member should never reveal their personal email address to a student. Should a student discover a teacher/staff member's personal email address and send mail to it, the message(s) should immediately be forwarded to the staff member's supervisor AND the district I.T. Network Administrator. To make this policy clear, ALL email between staff/teachers and students should be sent from AND to accounts that end with "k12coffee.net." Any other email correspondence between staff members and students is expressly prohibited.
The reasons for this practice are extensive. The primary reason is to protect both the student and the staff member. If staff and students are using accounts other than those provided by the district, the district has no way to monitor and archive those messages.

Staff and Security Training
All adults that use k12coffee.net accounts are required to participate in email and network cybersecurity training and immediately report to the Director of Technology any perceived security event.
If problems arise using district supplied accounts, district IT personnel should be notified immediately to resolve the issue.

CHAT ROOMS, NEWSGROUPS, SOCIAL NETWORKS, E-MAIL
Students are not allowed to participate in chat rooms, newsgroups, social networks or e-mail not provided by CCSS using the CCSS network. Any circumvention or violation of this policy may result in disciplinary action. Teachers may request that students be allowed access to these resources, but the request must be made to the teacher's principal and then the principal request sent to the Director of Technology. Students that violate this policy may be subject to disciplinary action and when applicable the involvement of appropriate law enforcement.

Professional Use of Social Media for Staff
1. CCSS employees should treat professional social media and communication like a professional workplace. The same standards expected in CCSS professional settings are expected on professional social media sites.
2. All professional social media accounts will be associated with district provided and/or managed login credentials and privacy settings.
3. Users that establish a username and password for any CCSS approved social media/online subscription for use by a school or classroom shall provide the username and password to building administration and administer the resource as any other professional social media.
4. All social media tools must be vetted by the district prior to use by a CCSS employee and/or student.
5. Employees using professional social media have no expectation of privacy with regard to their use of district social media accounts.
6. Employees are responsible for protecting confidential information or PPI. No personally identifiable student information may be posted on professional social media sites, including student photographs, without consent of the students' parents/guardians. Use of student images and/or information is addressed later in the RUP. Employees should carefully abide by the provisions of that section of this policy.

7. Employees have an individual responsibility to understand the rules of the social media being used and act to ensure the safety of students. Employees are responsible for reporting use of social media not adhering to this agreement to building administration.
8. Employees are expected to use the TAP principle (Transparent, Accessible, Professional) in all social media usage.

Personal use of Social Media
1. The district recognizes that during non-work hours employees and students may participate in online social media. Employees should keep in mind that information produced, shared, and retrieved by them may be subject to district policies and is a reflection of the school community.
2. The personal social media presence should utilize the employee's personal email address and not his/her k12coffee account and should be completely separate from any professional social media presence.
3. CCSS employees should not communicate with students who are currently enrolled in CCSS schools on personal social media sites with the exception of a relative. If a staff member receives a request from a current CCSS student to connect or communicate through a personal social media site, he or she should refuse the request.

WEBSITES
The Director of Schools may use any means available to request the removal of personal websites that substantially disrupt the school environment or that utilize school district or individual school names, logos, or trademarks without permission.

Students
Though school personnel generally do not monitor students' Internet activity conducted on non-school district devices during non-school hours, when the student's on-line behavior has a direct and immediate effect on school safety or maintaining order and discipline in the schools, the student may be disciplined in accordance with board policy (see the student behavior policies in the 6.300 series). Any device connected to the district network may be monitored by district personnel.

Employees
Employees' personal websites are subject to policy 4.406, Use of the Internet

Volunteers
Volunteers are to maintain an appropriate relationship with students at all times. Volunteers are encouraged to block students from viewing personal information on volunteer personal websites or on-line social networking profiles in order to prevent the possibility that students could view materials that are not age-appropriate. An individual volunteer's relationship with the school district may be terminated if the volunteer engages in inappropriate online interaction with students.

Cyberbullying
1. Cyberbullying will not be tolerated. Harassing, disrespectful comments, or comments which could be reasonably construed to incite an argument or are intended to belittle another person, denigrating, impersonating, outing, tricking, excluding, and cyber stalking are all examples of cyberbullying. Don't be mean. Don't send emails or post comments with the intent of scaring, hurting, or intimidating someone else.
2. Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In some cases, cyberbullying can be a crime. Remember that your activities are monitored and retained.

Usage of student images (photos and/or videos)
1. The CCSS encourages students to become active participants in their education. As a result, we may publish photos and/or videos of students on web resources controlled by the district, as well as print media such as district publications and programs. Note: consent to use student photos and/or videos is assumed by the district unless the parent/guardian opts out in accordance with option 2 below.
2. Note: To opt out of the district using the student's image and name, a guardian must provide written notification to the principal at your student's school that you do not give consent for images of your student to be used in district resources and print media. Acknowledgement of this procedure is included in the RUP Acknowledgement form included in this

RUP. Please be aware that teachers' district social media accounts are considered "district resources" for the purpose of this RUP.

DOCUMENTS, FILES and SOFTWARE

Students and staff should not alter, copy, move or delete any files, or access any file that they do not have permission to access. Programs, games, media or other files shall not be downloaded and installed on any CCSS computer system without the supervision and permission of CCSS technology department.

Google Drive

Staff and appropriate groups of students will have access to Google drive for storing school related documents. Files and content that is stored in Google Drive will adhere to all of the policies of this RUP.
Under no circumstance may software purchased by the school district be copied for personal use.
Users must back up locally stored (not on the district network or Google Drive) data and other important files regularly. It is the responsibility of the user to ensure that their files are backed up. District IT staff can assist any user needing help with this process.

PERSONAL DEVICES

While personal computers, electronic devices and digital storage media can be beneficial to the educational process, such items also have the capacity to become distractions and to convey material that is unsuitable for the school environment. Therefore, staff and students may use personal computers, electronic devices and digital storage media only with the permission of a supervising CCSS staff member or approved CCSS representative for the duration of the project. A student may NOT use previously mentioned equipment on campus on their own accord. When brought onto school property, these devices are subject to search and may be confiscated pending review and students may be subject to disciplinary action and, when applicable, the involvement of appropriate law enforcement.

In addition, anyone who uses school district computers or electronic devices or who accesses the school network using personal devices or the Internet using school district resources must comply with the policies of this RUP. These rules are intended to clarify expectations for conduct but should not be construed as all-inclusive. Furthermore, all students must adhere to the CCSS Guidelines as set forth in the Student Code of Conduct. All students must be trained about appropriate on-line behavior as provided in policy 4.406, Use of the Internet.

Because some incidental and occasional personal use by employees is inevitable, the district permits infrequent and brief personal use by employees so long as it occurs on personal time, does not interfere with school district business, and is not otherwise prohibited by board policy or procedure.

Artificial Intelligence (AI)

Privacy & Security

AI systems should be used in ways that respect the privacy or sensitive information of oneself or others. AI systems should not be used to access or share private or sensitive information about oneself or others, or include PPI in AI prompts. Users should not send or use in a prompt anyone's personal information like addresses, birthdays, phone numbers, or anything else that might be used to identify you or someone else to an AI tool. Staff should monitor student use to ensure that student data is not shared and appropriate consent and safeguards are in place to protect sensitive information. The use of AI tools must be in compliance with the resource's Terms of Service and the Children's Online Privacy Protection Act (COPPA). All AI tools used with students must also meet Family Education Right to Privacy Act (FERPA) requirements, allowing for parental control of student data.

Ethical Use

Staff

All staff are expected to model ethical behavior when using AI tools with students. Staff are responsible for accuracy (i.e. potential biases or limitations) and appropriateness of AI or other technology used. If AI generated work is utilized,

including AI generated communication to stakeholders and preparation or presentation of lesson content, staff should use the proper citation of the source. Staff must adhere to the CCSS Artificial Intelligence (AI) Policy.

Students
AI tools that are used by students should be used in ways that support learning, rather than ways that encourage academic dishonesty, such as plagiarism or cheating. Submitting AI generated work that you represent as your own will be considered academic dishonesty. When AI generated work is utilized, students should cite the source properly.

Students should not use AI tools without the express permission of the teacher.

Staff and students must adhere to the CCSS Artificial Intelligence (AI) Policy. Students should not use AI, or other technology, to generate anything that disrupts or disparages the District or any individual or group of people. The use of AI tools must be in compliance with the resource's Terms of Service.

Analyzing AI
Staff and Students should evaluate anything generated by AI for accuracy and appropriateness. All users should verify the information provided by AI or other technology resources and consider potential biases or limitations. Users will need to be careful of misinformation (something that is wrong) and disinformation (something that is wrong on purpose) in anything that is created with these tools. Identifying the difference between what is true and what is not becomes even more important when using AI tools.

Digital Well-Being
Staff and students should use AI tools and other technology thoughtfully to maintain a healthy balance with technology use in the educational process. AI systems might lack empathy and emotional intelligence and/or provide misleading or inaccurate information; therefore, staff should take into consideration the impact on student well-being when using AI, or any other technology.

Reporting Concerns
If staff or students identify potential biases or issues with AI systems or notice unethical or inappropriate use of AI, they should report their concerns to school administrators or teachers.

WARRANTY
Coffee County School District makes no warranties of any kind, whether expressed or implied, for the technology resources it provides. The district will not be responsible for damages suffered by students in the use of technology resources. This includes the loss of data, interruption of services, and access to inappropriate content online.

INTERNET SAFETY

It is the policy (4.406) of Coffee 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 direct electronic 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)] and Tennessee Department of Education requirements.

Coffee County Schools recognizes the importance of keeping children safe online. To address this issue, the district will provide the following:

Internet Training to Students

Internet safety training to students in K-12 is a part of their regular instruction. Resources will be provided to classroom teachers and instruction time will be allotted. Education about safe and appropriate online behavior will be integrated into the K-12 curriculum and instruction. Students need to learn how to avoid inappropriate content and unwanted contacts from strangers while online as well as appropriate behavior on social-networking and chat-room web sites and the dangers of cyberbullying and to learn about protecting personal information.

Supervision and Monitoring

All members of the Coffee County School System staff are responsible to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet Protection Act.

Evaluation and Review

The district will annually review its Internet safety program to make such adjustments as necessary. Appropriate personnel will review and evaluate all aspects of the Internet Safety Policy and program annually and will recommend revisions as needed.

Professional Development Opportunities for Teachers and Staff in District

(1)Professional staff development will be provided in the following areas: Internet Safety in the Classroom, Curriculum Design, Internet Usage for Lesson Planning and Content, Usage of Digital Media and other appropriate technologies that will enhance or secure the learning environment of Coffee County Schools..

(2)Opportunities for faculty and staff to attend technology professional development workshops, conferences or other appropriate venues will be offered.

Our system will provide on-site, ongoing professional development for all faculty and staff, throughout the school year. This will be accomplished by scheduling in-service opportunities and after-school training to promote effective integration of technology in the classroom and library which will lead to student improvement and network security.

Assessment of the effectiveness of professional development will be measured by analyzing student achievement scores, classroom grades, teacher observations, and by sending periodic surveys to faculty and parents. A needs assessment will be conducted to sustain professional development activities that integrate technology effectively for the next school year.

Parental Involvement:

Student Learning is maximized through familial or parental involvement in their schooling. However, family members may have very different levels of knowledge about instructional technology, and therefore varying capacity to become involved in a technology integrated learning process. Some parents do not understand the impact technology will have on their child's education as well as their child's post-high school employment prospects. In fact, many parents have a greater fear and misunderstanding of technology than do their daughters and sons. It is imperative to involve family members in the development of a school's technology plan and establish partnerships and include them in discussions and decisions. If parents are not involved, they may well oppose the plan based on fear rather than informed opinion.

The following are strategies that may be used in gaining parental involvement:

• Provide programs and/or speakers who can help parents, grandparents, caregivers, and community stakeholders understand how important it will be in the future for their children to be competent in safe technology use.

• Focus efforts to diminish parents' misconceptions, strengthen their technological awareness, and at the same time allow them to discover the potential of safe technology resources for their own uses.

• E-mail addresses of staff will be made available to parents and internet school sites will encourage communication between parents and teachers as well.

• Parents, grandparents, caregivers, and community stakeholders may be invited to attend the same meetings and training on safe technology usage that are held for the staff. As all participants are empowered with knowledge, they become more committed. As parents, grandparents, caregivers, and community stakeholders become better acquainted with teachers, they become more supportive.

Coffee County School System Student Responsible Use Policy (RUP)rev.2024

Acknowledgement /Parent Permission Form

I (student name) _____ have read and agree to comply with the Coffee County School System Responsible Use Policy. I understand that any violation of this policy may result in disciplinary action and the removal of computer/network access privilege.

Student School _____

Student Signature _____
(or electronic acknowledgement)
Date _____

Parent/Guardian Acknowledgement and Permission

As a parent or legal guardian of the above student, I understand that the Coffee County School System provides my student with internet access and access to digital resources. I understand that CCSS has implemented technology protection measures including filtering and monitoring to prevent students from accessing inappropriate materials on the Internet, but that such measures may not be one hundred percent effective at all times and it is impossible to restrict access to all controversial content. With this understanding I grant permission for my student to access the Internet. I also understand that CCSS provides my student with robust digital resources for classroom instruction that have been found to meet the Federal Trade Commissions' (FTC) regulations in regard to the Child Online Privacy Protection Act (COPPA). Some of these resources may require student login credentials, which I authorize at the district's discretion. A list of district-approved websites can be found at the district's website at www.coffeecountyschools.com under the COPPA heading. I understand that the CCSS RUP restrictions and guidelines are necessary components in protecting my child from exposure to inappropriate materials and from participating in inappropriate activities. I understand that any violation of this policy may result in disciplinary action and the removal of computer access privilege for my student.
My child can be featured in local broadcast and print media, on the school or school district website, and in district publications and programs. Only photos and name will be given.
I understand that if I do not want my student featured in any of the above media, I will need to provide a written notice to the administrator of the school my student is attending.

Printed Name of Parent/Guardian _____

Signature_____ Date _____
(or electronic acknowledgement)

Digital Resources Parent/Guardian Form

Coffee County School System (CCSS) students will be using a variety of digital resources to enhance their learning experience. Although these applications are widely used by the education community and support their use in K-12 institutions, their Terms of Service state that due to the Federal Law COPPA, any users under the age of 13 and some under the age of 18 must obtain explicit parental permission to use them.

All digital resources have been and will continue to be thoroughly examined by experienced educators that comprise our Digital Learning Team. As these sites are instrumental in the development of the curriculum, we are asking that you and your student please review the permission form below and complete it. Should you not want to give permissions or your expectations change, you must provide notification in writing to the school office your student attends. If you do not give your student permission to use these web tool applications, an alternative assignment will be provided. All of these tools must be used in accordance with the CCSS Responsible Use Policy, even if the student uses the tools outside of school on their own device.

I have read this permission slip and the CCSS Parent-Guardian Computer Responsible Use Agreement.

YES, I give permission for my child to use these web tools to enhance their learning experience. I understand that if I do not give permission I must provide notification in writing to the school office where my student attends and an alternative assignment will be provided.

Student Name Printed:

_____

Student Signature:
(or electronic acknowledgement)

_____

Parent/Guardian Signature:
(or electronic acknowledgement)

_____

Date: _____

Coffee County School System Staff Responsible Use Policy (RUP)rev.2024

Acknowledgement Form

By signing below, I acknowledge that I have read and understand the Coffee County School System Responsible Use Policy and Internet Safety Policy and agree to follow this policy governing the use of Coffee County's network and computer systems and if so assigned, provide approved Internet Safety training as outlined in the RUP. I understand that I must only use websites that the district has approved with my students and that I must follow the policy to protect student Protected Personal Information (PPI). I understand that violation of the CCSS RUP policy could result in disciplinary/legal action in accordance with the RUP and the Coffee County Board of Education policies.

Name (printed)_____

Signature _____
(or electronic acknowledgement)

Date _____

School or current assignment _____