ACCEPTABLE USE OF COMPUTER TECHNOLOGY AND RELATED RESOURCES

2025-2026

Randolph County School System

Randolph County School System Board of Education
Mr. Ra'Mel Thomas (Chairman)
Mr. Jack Fowler (Vice-chairman)
Mr. Rodney Burks
Mr. Henry Cook
Mrs. Dymple McDonald

Superintendent
Dr. Tangela Madge

Director of Technology
James Cobb

The Randolph County School System does not discriminate on the basis of race, color, national origin, sex, disability, or age in admission to its program services or activities. AdditionAL information can be found at https//www.sowegak12.org. The Randolph County School System does not discriminate against its hiring or employment practices.

ACCEPTABLE USE OF COMPUTER TECHNOLOGY AND RELATED RESOURCES

1.1.0 Employee and Student Acceptable Use of Technology and Related Resources

1.1.1 General – To facilitate achieving a quality education for its students, it is the policy of the Randolph County Board of Education (Board) to provide all students and employees with opportunities to access a variety of technological resources to fully prepare students for life beyond the K-12 educational environment. A large and varied technological environment requires that technology use by employees and students be legal, ethical and safe. Technology use must be consistent with the educational vision, mission, and goals of the Board.

a. The Board employs a Director of Technology (DoT) to provide technological support at the school system and school levels.

b. School computers, networks, e-mail and Internet access are provided to support the educational mission of the Randolph County School System (RCSS) and are to be used primarily for school-related purposes. Personal use of school computers must not interfere with the employee's job performance or student's academic performance, must not violate any of the rules contained in Board policy, procedures, or other like directives and must not damage the school's hardware, software or communications systems.

c. "Community Use" of wireless internet resources may be permitted through the district's guest wireless network providing that the use does not violate any applicable laws or board policies, procedures, and like directives and does not affect the educational environment. The RCSS reserves the right to suspend community use at any time without notice.

d. The term "system" for purposes of this policy may mean the totality of resources serving the central office and schools, the totality of resources within a school, or the totality of resources accessible by a given workstation or application.

1.1.2 Policy Rules – The goal of using the school's computers, local area network, the system's wide area network and the Internet is to bring available educational resources to both students and staff and to facilitate diversity and personal growth in technology, information gathering skills, and communication. Providing these resources is intended to promote educational excellence by linking individuals and classrooms to global resources to facilitate resource sharing, innovations, and communications. These rules establish usage

appropriate for an educational setting and require users to act responsibly and accountably.

1.1.3 Copyright Law – It is the obligation and intent of the Board to comply with the copyright laws of the United States. Board employees and students shall use technology resources in accordance with Board policies and procedures, as well as local, state, and federal laws and guidelines governing the use of technology and its component parts.

a. Individuals are responsible for keeping unauthorized, copyrighted software of any kind from entering the local area network or wide area network via the Internet or other means. This includes loading, copying, or downloading of any programs, games, electronic media, etc.

b. If a single copy of a software package is purchased, it may only be used on one computer at a time. Multiple loading or "loading the contents of one disk on multiple computers" (1987 Statement on Software Copyright) is not allowed.

c. If more than one copy of a software package is needed, a site license, lab pack, or network version will be purchased. DoT will work with appropriate district personnel to determine how many copies will be purchased for the location.

d. The DoT is authorized to sign license agreements for a school within the district or the district itself.

e. Employees may be held personally liable for any actions that violate copyright laws.

1.1.4 Network Accounts – Network user accounts are provided to faculty, staff, and students. These accounts are utilized to provide access to district resources. Wherever possible, the district synchronizes these accounts with third party systems to allow easier access for our faculty and students.

a. All staff may receive network accounts after Board approval of the personnel. A potential employee may be granted an account prior to the first day of employment if requested by the principal, supervisor or Superintendent in writing to the DoT. For requested accounts, the principal/supervisor or Superintendent will be responsible for notifying the DoT if employment is not approved by the Board.

b. Network accounts for contract or temporary employees may be requested in writing to the DoT by the principal, supervisor, or Superintendent. Requests must be accompanied by a copy of the contract and description of duties. For requested accounts, the

principal/supervisor/Superintendent will be responsible for notifying the DoT if employment ends prior to the expiration of the contract period.

c. Student network accounts are generated based on pertinent information pulled from the district's student information system.

d. The DoT may provide temporary or special use accounts at his/her discretion provided that they do not violate any applicable law or board policy.

e. Network accounts should never be shared with other users, or outside organizations. Doing so is a direct violation of this policy. If an account has been compromised, it should be reported to the technology department immediately.

f. Network accounts may be disabled or otherwise restricted for disciplinary or other reasons at the request of the applicable principal or supervisor or at the discretion of the DoT, Superintendent, or his/her designee.

g. When an employee user is terminated or separates employment, or a student user is unenrolled from RCSS, the access to systems and applications shall be immediately terminated unless continued access is approved in writing by the RCSS Superintendent and the DoT. Employee User's work records and data and Student User's data and records stored locally or on Board servers shall be preserved for 30 days unless longer retention is required by pending or threatened litigation or applicable records retention policies. Access to stored data must be requested in writing and approved by the RCSS Superintendent and the DoT.

1.1.5 Data Networks – The RCSS provides multiple data networks for the use of the faculty, staff, and students for the purpose of meeting the educational vision, mission, and goals of the Board. Use of the data networks may be suspended or revoked as deemed necessary by the DoT, Superintendent, or his/her designee.

a. Users may utilize only those computers and devices approved by the RCSS Technology Department on the wired district network or the internal wireless network and are prohibited from connecting any device to the physical network or network equipment without the knowledge and consent of the DoT.

b. Personally owned cellular devices may only be connected to the provided guest wireless network or BYOT network.

1.1.6 Privacy – All technology resources, including network and Internet resources, e-mail systems, and computers or other access devices owned, leased, or maintained by the Board are the sole property of the Board. Authorized Board personnel may, at any time and without prior notice, access, search, examine, inspect, collect, or retrieve information of any kind from the Board's technology resources, including computer or related equipment, files, and data, to determine if a user is in violation of any of the Board's policies, rules, and regulations regarding access to and use of technology resources, for or in connection with any other matter or reason related to the safe and efficient operation or administration of the school system, or for any other reason not prohibited by law. Users of school system technology resources have no personal right of privacy or confidentiality with respect to the use or content of such resources. The Board reserves the absolute right to access and monitor all messages and files on Board equipment. Employees and students shall have no expectation of privacy with regard to such data. Spam or obscene e-mail that bypasses the school system filtering should be reported to the DoT.

1.1.7 Data Governance – The Superintendent is authorized to establish procedures governing the storage, use, and sharing of data maintained electronically by the school system. Such procedures shall comply with applicable state and federal law and shall include provisions for data security (including physical security measures), access controls, quality control, and data exchange and reporting (including external data requests, and third-party data use). Nothing in this policy or in any procedures authorized hereunder creates or expands any entitlement to confidentiality of records beyond that which is established by law or specific Board policy.

1.1.8 Any unauthorized access, use, transfer, or distribution of Board data by any employee, student, or any other individual may result in disciplinary action (up to and including termination for employees) and other legal action.

1.1.9 Rules of Behavior on System Networks or Equipment – Employees and students are responsible for their behavior on school computer networks just as they are in other aspects of their jobs. Employees and students who misuse the school system's technology may be subject to denial of computer usage, monetary charges, and/or other disciplinary actions. Violation of civil and/or criminal law relating to technology and its use may result in the notification of law enforcement officials. Specific guidelines include those below.

a. Employees and students may not access, transmit, or retransmit material which promotes violence or advocates destruction of property including, but not limited to, access to information concerning the manufacture of destructive devices such as explosives, fireworks, smoke bombs, incendiary devices, etc.

b. It is forbidden to advocate or promote violence or hatred

against a particular individual or groups of individuals or advocate or promote the superiority of one racial, ethnic, or religious group over another. Production or dissemination of hate mail, obscenity, harassment, inflammatory material, chain letters, discriminatory remarks, disrespectful language, and other behaviors disruptive to the educational environment are prohibited on district resources. This includes, but is not limited to:

i. Harassing, threatening, insulting, bullying or attacking others.

ii. Using the system network to create dissension or conflict.

c. The RCSS network may not be used to access, transmit, or retransmit any information containing pornographic or other sexually oriented material or language (pornographic means pictures or writings intended to stimulate erotic feelings by the description or portrayal of sexual activity or the nude form). Accessing, transmitting, or retransmitting may include but may not be limited to:

i. Viewing pornography on the computer.

ii. Conducting sexually explicit discussions with Internet partners at any time of the day.

iii. Sending, displaying, viewing or downloading offensive messages, pictures or movies.

iv. Using obscene or profane language.

d. Individuals may not use technology for illegal activities including gambling, plagiarism of materials found on the Internet and creating illegal materials such as counterfeit money, fake identification, etc.

e. Users may not purchase or install software or other digital media to be used on system networks and/or individual workstations within the system without express written permission of the DoT. For purposes of this policy, “install” is defined as copying software of any kind in any form, downloading software from the Internet, and/or loading software from any external source, including personal copies, onto an individual computer, a network directory, or mapped drive.

f. It is forbidden to use or possess bootleg software (bootleg software means any software which has been downloaded or is otherwise in the user’s possession without the appropriate registration of the software

including the payment of any fees owed to the owner of the software). Illegal, unauthorized, or unlicensed copies of software must not be used on school system equipment.

g. Users may not commit or attempt to commit any willful act involving the use of the network which disrupts the operation of the network or compromises its security within the school district or any network connected to the Internet including the use or attempted use or possession of computer viruses.

h. Individuals shall not transmit personal and confidential information concerning students or others to those not authorized to receive such information. Care must be taken to protect against negligent disclosure of such information.

i. It is forbidden to use passwords improperly or negligently or for employees to use or modify another's passwords. No message should be transmitted without the sender's identity. The transmission of messages with anonymous or fictitious names is prohibited. Accounts are to be used only by the authorized/registered user and for the intended purposes of the account.

j. District computers may not be moved off campus unless authorized by the administrator and DoT.

k. District devices assigned to employees may be taken off campus upon completion of a Faculty Device Contract.

l. Individuals may not advertise and solicit on the school network or offer or provide products or services on system networks. District internet and e-mail accounts may not be used for commercial purposes or personal or political gain.

m. Users shall not intentionally modify files, other data, or passwords belonging to other users. Users shall not misrepresent other users on the Internet.

n. Individuals are responsible for any hardware and/or software damage to the computers or the network caused by inappropriate behavior while using the system. These include, but are not limited to, tampering with the equipment, altering programs and/or files, installing programs without authorization, or reconfiguring any part of a computer.

1.1.10 System Integrity and Control – To assure the integrity and control of system resources and capability, the DoT, Technology Department Staff and Media Specialists will be the only persons authorized to access original software

disks at a given school location.

o. To assure compliance with copyright and licensing requirements, only members of the District Technology Department may install software to be used on system networks and/or individual workstations within the system. Staff should contact technology for assistance with software installation. For purposes of this policy, "install" is defined as copying software of any kind in any form, downloading software from the Internet, and/or loading software from any external source, including personal copies, onto an individual computer, a network directory, or mapped drive.

p. Individuals are not authorized to make copies of any software or data without the knowledge and permission of the DoT. Any questions about copyright provisions should be directed to the DoT. Illegal, unauthorized, or unlicensed copies of software must not be used on school system equipment. Any copies will be subject to the district's data governance policy and procedures.

q. District owned software cannot be installed on personal devices unless specifically allowed by the software's licensing agreement.

1.1.11 Application of Policy – See Below

a. All Board technology resources, regardless of purchase date, location, or fund sources (including donations), are subject to this policy.

b. Employees who misuse the school system's technology may be subject to denial of computer usage, monetary charges, reprimands, and/or loss of employment.

c. Students who misuse the school system's technology may be subject to denial of computer usage, monetary charges, and/or other disciplinary actions.

d. The Superintendent or his designee will prepare procedures for implementing this policy at the system and school levels.

e. The administration of each school will be responsible for reviewing these policies at the beginning of each year with the faculty and staff and with individual employees who are hired after the initial review. The administration must have faculty and staff members sign this policy indicating they are aware of the rules and have reviewed them. This policy may be available online and may require acknowledgement online before further access is granted. The administration is encouraged to have a separate review of copyright law each school year.

f. The legal and ethical practices and responsibilities of appropriate use of technology resources will be taught to all students in the system during lab orientation, by homeroom teacher, media specialist, etc.

g. Individuals are expected to report any violations of this policy and/or problems with the security of any technology resources to the Principal and/or DoT.

h. Any questions about this policy, its interpretation, or specific circumstances shall be directed to the DoT.

1.1.12 Disclaimer of Liability –The Board makes no warranties of any kind; either expressed or implied that the functions or the services provided by or through the Board's technology resources will be error-free or without defect. The Board will not be responsible for any damage users may suffer, including but not limited to loss of data or interruption of service.

1.1.13 Electronic Mail – Electronic E-mail is available for the support of educational, instructional, extracurricular, and administrative activity. With that purpose in mind, electronic mail accounts are available to employees and students according to the following guidelines:

a. Staff will receive e-mail accounts when their network accounts are created.

b. Students receiving e-mail accounts must use these accounts for instructional purposes only and, while at school, should only use mail accounts provided by the district when using the school system's network or school-owned technology device.

c. All staff and student e-mail accounts are subject to monitoring and acceptable use policies.

d. The Board cannot guarantee the privacy, security, or confidentiality of any information sent or received via electronic mail. The Board will use a filtering device/software to screen e-mail for spam and inappropriate content.

e. District email and other electronic communications are subject to long term logging and/or archiving as deemed appropriate by the Superintendent and DoT.

1.1.14 Internet – The intent of the Board is to provide access to resources available via the Internet with the understanding that faculty, staff, and students will access and use only information that is appropriate, beneficial, and/or required for various curricular or extracurricular activities or staff duties.

Teachers will screen resources that will be used in the classroom for instructional content prior to their introduction. Board policies and procedures apply to the use of the Internet.

a. Internet access is provided to allow students, faculty and staff to conduct research and access resources. Users gaining access to the Internet agree to conduct themselves in a considerate and responsible manner. By signing the Code of Student Conduct and the Student/Parent Device Agreement Form for each student in the household, legal custodians/parents provide written permission for their child to have access to the Internet and network resources.

b. The Board provides technology protection measures that include blocking or filtering Internet access to visual depictions and text that are obscene, pornographic, or harmful to minors. These measures cannot be considered 100% effective. Teachers must preview websites being used for instructional purposes and observe students using the Internet. Teachers are responsible for monitoring and overseeing student use of computers and online resources in accordance with this Acceptable Use Policy, and for educating students about digital safety and ethics as well as integrating into their teaching digital citizenship in the classroom. If a student encounters inappropriate content online, they are to immediately close the browser and report the incident to the teacher. Sites that are deemed inappropriate or a disruption of the learning atmosphere should be reported to the DoT. Teachers may request blocked sites be opened which they feel are appropriate and needed for instruction by contacting the Technology Department.

c. Sites found to disrupt the learning atmosphere by consuming excessive internet bandwidth may be blocked or otherwise limited at any time without notice.

d. Network users are prohibited from accessing external networks or alternate Internet service providers while within the RCSS's internal network unless expressly authorized by the Superintendent or DoT and properly protected by a firewall, other appropriate security device(s), and appropriate filtering software. This prohibition includes, but is not limited to, VPN or other technologies that attempt to bypass district filters/security, cellular "hot spots", cellular data plans, etc.

e. All school rules and guidelines for appropriate technology use shall apply to use of the Internet. Because communications on the Internet are often public in nature, all users must engage in appropriate and responsible communications with particular regard to avoiding disruption of the educational environment.

f. Employees and students should be aware that posting of personal

information of any kind about themselves or others is prohibited. Personal information includes home addresses, work addresses, home phone numbers, social security numbers, etc.

1.1.15 Artificial Intelligence Acceptable Use - RCSS acknowledges that technology is ever-changing and has a tremendous impact on our global society, local community, and classrooms. Artificial intelligence (AI), including generative forms of AI, is becoming more a part of our everyday lives. It is our responsibility to educate and train students to utilize AI in an ethical and educational way. Therefore, RCSS is not banning the student or teacher use of AI, but each student will need to be aware of the limitations and guidelines of its usage:

a. RCSS student email accounts and Chromebook will have access to specific open AI software, such as ChatGPT, however, they can be blocked due to data and security concerns.

b. Any misuse of AI tools and applications, such as hacking or altering data, is strictly prohibited.

c. Teachers may allow the use of AI for curriculum purposes. Access to specific websites will be granted on an as needed basis, adhering to specific data and privacy guidelines regarding age restrictions and usage.

d. College Board and Dual Enrollment college and university classes may have additional restrictions and limitations regarding the use of Artificial Intelligence.

e. Students who use AI software with a personal device and/or personal credentials should do so at their own risk - acknowledging that each platform is collecting various forms of data.

f. Students must acknowledge the use of AI in any capacity related to their schoolwork: text, image, multimedia, etc.

g. The use of AI could be subject to the Academic or Dishonesty Policies at each school or at the teacher's discretion.

h. Students should acknowledge that AI is not always factually accurate, nor seen as a credible source, and should be able to provide evidence to support its claims.

i. All users must also be aware of the potential for bias and discrimination in AI tools and applications.

1.1.16 Learning Management Systems – The school system provides methods

for students to upload and send assignment files to teachers.

1.1.17 Mass Electronic Notification Systems -

a. General. The RCSS maintains mass electronic notification systems for the purpose of facilitating the dissemination of educationally-related information to stakeholders. It is the hope of the Board that each school will use such systems for distributing emails and pertinent announcements to parents and guardians.

b. Uses. The mass electronic notification system from RCSS will be used for educational and informational purposes only and in accordance with all Randolph County policies and procedures. All submissions/postings to the program will be written and released by approved webmasters and/or administrators.

c. Membership. Because mass electronic notification systems maintained by RCSS are intended for informational purposes for stakeholders, information for membership will be distributed by each of the schools within the school system and on the school system websites.

d. Disclaimer. The RCSS and its employees cannot be held responsible for postings through mass electronic notification systems including, but not limited to, acts of omission, accidental misinformation, or information that may come into the possession of unintended parties or individuals.

1.1.18 District Devices and Equipment – All purchases of technology-related devices and equipment for the district, regardless of funding source, must be coordinated through the technology department in order to ensure inventory integrity and safeguard network management, control, and compatibility. Only devices and equipment approved by the DoT may be purchased with district or donated funds. Any technology-related donations to the district must be coordinated through the DoT before being accepted. All RCSS students will be allowed to use devices while at school and a charger in each school, or upon successful enrollment in RCSS, and the device will travel with the student from year to year with that school until graduation, device refreshment, or withdrawal from RCSS.

1.1.19 Personal Devices – RCSS promotes a 1:1 shared device initiative while at school. As such, a wireless network is provided for cellular devices and guest use only. School-issued devices will authenticate to the network automatically. All personal cellular devices and guest devices should utilize the BYOT or Guest wireless network.

1.1.20 Web Sites (District, School, and School-Sponsored Activities) – The District provides a website platform used by all district entities to maintain consistency. Because District web sites are globally available and represent the

community at large, webmasters are required to adhere to all acceptable use standards and present an appropriate and positive image.

1.1.21 Students/parents/staff of the Randolph County School System will be held financially responsible for any damage and will be billed for full replacement costs for stolen, damaged, lost equipment. Remember, it is the parent's/student's/staff's responsibility to report the theft to the proper police and school authorities immediately upon incident. Any damage should be reported to the teacher, Director of Technology, or other administrator immediately. After the investigation, if a device is deemed stolen, the school will make a determination regarding a replacement device. Please see the approximate cost table at the end of this document.

SOCIAL MEDIA POLICY

Purpose for Social Media Guidelines

The Randolph County School System (RCSS) recognizes that access to technology in school gives students, parents and teachers greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. Effective communication with colleagues, students and families is vital for a thriving school environment where all stakeholders feel heard and engaged.

To this aim, the Randolph County School System has adapted the following guidelines to provide direction for faculty, staff, and students when participating in online social media activities. Whether or not an employee chooses to participate in a blog, wiki, online social network or any other form of online publishing or discussion is his or her own decision. Free speech protects individuals who want to participate in social media, but the laws and courts have ruled that school districts can discipline employees if their speech, including personal online postings, disrupts school operations.

These guidelines have been formed as a resource for you. It is important to create an atmosphere of trust and individual accountability. Keep in mind that information produced by RCSS employees is a reflection on the entire District and is subject to the District's Acceptable Use Policy. Personal postings, even if marked private, may also be subject to relevant RCSS policies and procedures, as well as to relevant local, state and federal laws. By accessing, creating or contributing to any blogs, wikis, podcasts or other social media for classroom or district use, you agree to abide by these guidelines. Please read them carefully before participating in any social media application.

What is Social Media?

Social media is the collective of online communications channels dedicated to community-based input, interaction, content-sharing and collaboration.

Tools include, but are not limited to:
• Blogs (Blogger,WordPress, etc.)
• Wikis (Wikispaces, Google Sites, etc.)
• Social Networking sites (Facebook, Ning, MySpace,YouTube, LinkedIn, etc.) • Photo and Video Sharing sites (YouTube, Flickr, etc.)
• Social Bookmarking (Diigo, Delicious)
• Podcasting and Vodcasting

Personal Responsibility

• Randolph County School System (RCSS) encourages district employees with a personal online presence to be mindful of the information they post. Your online behavior should reflect the same professional and personal standards of honesty, respect and consideration that you use face-to-face and in work-related settings.

• Please note that even if you delete personal information, it still may be stored on the website's server for a longer period of time. Information that is marked "private" rarely is private on the Internet. It is very easy for "friends" to copy and paste information about you and send it or forward it to others, for example. There is no realistic expectation of privacy on the World Wide Web.

• The lines between public and private, personal and professional are blurred in the digital world. By virtue of identifying yourself as a RCSS employee online, you are now connected to colleagues, students, parents and the school community. Use these connections wisely and well. You should also ensure that content associated with you is consistent with your work at RCSS and your role as a public school/State employee.

• It is your responsibility to familiarize yourself with the appropriate security settings for any social media (personal or professional) that you may use. Be sure that the settings are such that your intended audience may only view any personal content. Be aware that, even if your privacy settings are set properly, it is still possible for anyone who you've allowed to see your profile to copy and paste text and send it to someone else. It is also easy for others to "tag" or identify you in photos that they publish with or without your knowledge and permission. Similarly, if you enable settings such as Facebook's ability to allow "friends of friends" to view your content, it is extremely likely that unintended viewers will have access to pictures and other personal content.

• It is inappropriate to use e-mail, text messaging, instant messaging or social networking sites to discuss with a student a matter that does not pertain to school-related activities. Appropriate discussions would include the student's homework, class activity, school sport or club or other school-sponsored activity. Electronic communications with students are to be sent simultaneously to multiple recipients, not to just one student, except where

the communication is clearly school-related and inappropriate for persons other than the individual student to receive (for example, e-mailing a message about a student's grades).

• Engaging in personal social-networking friendships on MySpace, Facebook or other social networking sites is prohibited with students. A recommendation for staff to respond to "friend" requests on their personal pages is:

If you are a student or parent requesting to be my "friend," please do not be surprised or offended if I ignore your request. As an employee of Randolph County School System, District procedures and practices discourage me from "friending" students on my personal pages. I would encourage you to friend our school's (and/or classroom's, department's, the Randolph County School System's Facebook pages, etc.)

• Material that employees post on social networks that is publicly available to those in the school community must reflect the professional image applicable to the employee's position and not impair the employee's capacity to maintain the respect of students and parents/guardians or impair the employee's ability to serve as a role model for children.

Professional Responsibility

• While social media can be a powerful communication tool and an educational tool for students and parents, RCSS employees are personally responsible for the content they publish online. Be mindful that what you publish will be public for a long time—protect your privacy.

• Remember that social media in the classroom is an extension of your physical classroom. What is inappropriate in your classroom should be deemed inappropriate online.

• Teachers who use social networking to interact with students and/or parents in an educational manner or as a communication tool must find ways to interact without giving students and parents access to their personal information and posts. Many social network sites allow you to create "groups" or "pages" where you can interact with students without giving them access to your personal account. Please see detailed Facebook guidelines for more information.

• When contributing online do not post confidential student information. Do not post pictures of any students on your personal sites.

• Use a RCSS provided e-mail as your e-mail contact for official or school-related pages. Do not use your RCSS provided e-mail as a username or e-mail contact for personal pages.

• Please remember that all RCSS policies and procedures, as well as relevant local, state and federal laws (copyright, fair use, Family Education Right to Privacy Act, personnel statutes, criminal statutes, etc) apply to social media communications.

Overall Guidelines for Using Social Media

The following are general guidelines for using social media whether personally or professionally.

Be Transparent

How you represent yourself online is an extension of yourself. Do not misrepresent yourself by using someone else's identity or misrepresenting your identity. Be honest about who you are, where you work and what you do.

Always a School Employee

Although the lines between public and private, personal and professional, can become blurred in the digital world, you will always be considered to be a RCSS employee. Whether it is clearly communicated or not, you will be identified as an employee of the School District in what you do and say online. If you don't want it on the 10 p.m. news or in the daily newspaper - don't share it online.

School Values

Represent RCSS district values. Express ideas and opinions in a respectful manner. All communications should be done in good taste. Build trust and responsibility in your relationships. Do not denigrate or insult others including students, staff, administrators, parents or other districts. Any online contributions must be in accordance with the appropriate policies, guidelines and relevant laws. Consider carefully what you post through comments and photos. A violation of these policies, guidelines and/or relevant laws could be regarded as a form of professional misconduct and may result in disciplinary action.

Build Community/Positively Represent School

Represent RCSS, the students and parents you serve in the best light. Respect the privacy and the feelings of others. Under no circumstance should offensive comments be made about students or colleagues (including administrators) nor the District in general. Negative comments about people may amount to cyber-bullying and could be deemed a disciplinary offense. Your posts and comments should help build and support the school community. Do not comment on nor forward unsupported information, e.g. rumors. You are responsible for what you and others post, even if on a personal page, so be certain it is accurate and supports your organization. It is a good idea to monitor your profile page to ensure that all material posted by others doesn't violate these guidelines. Once posted you can't take it back.

Other Online Activities

Part of the Internet's popularity is its many online diversions. Be careful of gimmicks or games that many websites use to increase web traffic. Examples can include risqué surveys or quizzes. Often comments or information thought to be shared in private are capable of being shared publically. Also, employees may be disciplined for using their online access for non work-related purposes.

Share your Expertise

Write what you know and be accurate. Add value to the discussion. Post something useful. Provide worthwhile information and perspective. A district's most valuable asset is its staff represented by its people and what you publish may reflect on the school. Speak in the first person with your own voice and perspective.

Respectful and Responsible

Employees, parents, and students reflect a diverse set of customs, values and points of view. Be respectful for others' opinions in your posts or comments. You are responsible for the content you post. Do your tags, descriptions and your image portray you and the District in a professional manner?

Own and Correct Mistakes

If you make a mistake, admit the mistake and correct it quickly. Share your error with your principal, Human Resources, or Superintendent so they can help address the issue effectively. Clearly state if you've corrected a previous post. Even though damage may be done, it is best to admit your mistake and correct it. Apologize if appropriate.

Confidential Information

Online postings and conversations are not private. Do not share confidential information whether it is internal school discussions or specific information about students or other staff. What you post will be seen by others and will be online for a long time. It can be forwarded or shared in just a few clicks. Do not write about colleagues or students without their expressed permission.

School Logos

Obtain written permission before using any school or district logo or image. School logos may only be used in a professional capacity. When using social media for RCSS or school-related purposes, please follow the RCSS Style Guide.

Posting Photos or Movies without Permission

Do not post or tag photos or movies of others without their permission. Do not use photos or movies taken at school without permission. Do not post photos or movies that contain students without parent consent.

Responding to Negative Comments and Criticism

How you respond to negative comments or criticism will say more about you and your character than what you post. When in doubt, it's best not to give it credibility by acknowledging it with a response publicly; perhaps a private response would be more appropriate. See the response guidelines for more information on responding to these types of comments.

Response and Post Regularly

To encourage readership, post regularly. Don't post to your blog and then not post for three weeks. Readers won't have a reason to follow you if they cannot expect new content regularly. Respond to other's posts. Answer questions; thank people even if it's just a few words. Make it a two-way conversation.

Spell Check and Abbreviations

Any online contribution should be well written. What you post will be online for the world to read. Follow writing conventions including proper grammar, capitalization and punctuation. Be cautious about using common abbreviations. While your circle of friends may understand what you are saying, you may have readers from across the world that won't understand. When in doubt, define the abbreviation at least once in a post or include a definitions page on your site.

Copyright and Fair Use

Respect copyright and fair uses guidelines. Share what others have said by linking to the source and using embedded content. Be sure to cite your source when quoting. When using a hyperlink, confirm that link goes where it should and that the content is appropriate. Keep in mind that copyright and fair use also applies to music. Do not post presentations or videos using popular music, or any music or art that you have not obtained the appropriate permissions for use.
For example, just because you've purchased something for personal use doesn't mean you've purchased the right to broadcast it to others online.

Personal Information

Be careful about sharing too much personal information. People often share personal information such as their pet names, their parents and children's names, where they grew

up, and more. This information may help a hacker guess your passwords. If you share that you will be out of town, a criminal may use this to target your home for a burglary. Do not share with a student your personal problems that would normally be discussed with adults. Be smart and don't share too much information.

Video

The Internet is becoming an increasingly popular educational tool and place to share personally created movies. You are responsible for all you do, say, and post online, including video. Anything you post online should represent you in a professional manner, as others will see you as connected to the School District. You should preview anything you show in your classroom in its entirety, prior to any student seeing it. Consult a supervisor if you feel the content may be questionable.

Staff-Student Relations

Employees are prohibited from establishing personal relationships with students that are unprofessional and thereby inappropriate. Examples of unprofessional relationships include, but are not limited to: employees fraternizing or communicating with students as if employees and students were peers such as writing personal letters or e-mails; personally texting or calling students, or allowing students to make personal calls to them unrelated to homework, class work, or other school-related business; sending inappropriate pictures to students; discussing or revealing to students personal matters about their private lives or inviting students to do the same (other than professional counseling by a school counselor); and engaging in sexualized dialogue, whether in person, by phone, via the Internet or in writing.

Employees who post information on Facebook, Instagram, MySpace or similar websites that include inappropriate personal information such as, but not limited to: provocative photographs, sexually explicit messages, abuse of alcohol, drugs or anything students are prohibited from doing must understand that if students, parents or other employees obtain access to such information and report this to the district, their report will be investigated by school and district officials.

Social Media Guidelines for Students

1. Social media venues are very public. What you contribute leaves a digital footprint forever, usually even after it is deleted. Do not post anything you wouldn't want friends, enemies, parents, teachers, or a future employer to see. Make sure what you post promotes a positive image to the world.

2. Follow the school's code of conduct when writing online. It is acceptable to disagree with someone else's opinions, however, do it in a respectful, constructive way. What is inappropriate in the classroom is inappropriate online.

3. Be safe online. Never give out personal information, including, but not limited to, last names, any phone numbers, addresses, birthdates, and pictures. Do not share your password with anyone besides your parents, and teachers if necessary.

4. Linking to other Web sites to support your thoughts and ideas is recommended. However, be sure to read the entire article prior to linking to ensure that all information is appropriate for a school setting.

5. Do your own work! Do not use other people's intellectual property, including pictures, without their permission. It is a violation of copyright law to copy and paste other's thoughts without proper attribution. When paraphrasing another's idea(s) be sure to cite your source with the specific web address. Verify you have permission to use the material or it is under Creative Commons attribution.

6. How you represent yourself online is an extension of yourself. Do not misrepresent yourself by using someone else identity.

7. Blog, wiki, and other online posts should be well written. Follow writing conventions including proper grammar, capitalization, and punctuation. If you have permission to edit someone else's work be sure it is in the spirit of improving the writing.

8. If you run across inappropriate material, that makes you feel uncomfortable, or is not respectful, tell the supervising adult right away.

9. Cyber bullying is not tolerated. What constitutes cyber bulling, the actions you should take to document cyber bullying if you feel you are a victim, and the actions that may be taken against participating individuals are clearly outlined in the student handbook.

10. Students who do not abide by these terms and conditions may lose their opportunity to take part in the project and/or access to future use of online tools.

Disclaimers

- Randolph County School System employees are highly encouraged to include disclaimers within their **personal** blogs that the views are their own and do not reflect on their employer. For example, "The postings on this site are my own and don't necessarily represent Randolph County School System's positions, strategies, opinions, or policies."
- This standard disclaimer does not by itself exempt Randolph County School System employees from a special responsibility when blogging.
- Classroom blogs do not require a disclaimer, but teachers are encouraged to moderate content contributed by students.

Adapted From:

Social Media Guidelines Wiki

Referenced Sites and Resources

Barrow County Schools: http://www.barrow.k12.ga.us/

Social Media Guidelines for Educators
(Facebook group): http://www.facebook.com/group.php?gid=80354045978

Social Media Guidelines for Schools - Andy Mann, Calhoun ISD
http://www.scribd.com/doc/28430149/Social-Media-Guidelines-for-Schools

Social Media Guidelines for Schools Wiki -
http://socialmediaguidelines.pbworks.com/ •

Social Media Suggestions:
http://blogs.stvrain.k12.co.us/helpdesk/2010/03/29/social-media-suggestions/

Think Social Media Guidelines: http://thinkingmachine.pbworks.com/Think-Social-Media-Guidelines

Quitman County School District: https://www.quitman.k12.ga.us/technology

Example of Social Media Guidelines
Parent Permission Form for Student Participation

Dear Parents:

This year, to help our students develop their reading and writing skills as well as cultivate our understanding of different people and cultures; our students are participating in using a variety of social media applications (blogs, wikis, podcasts) via the Internet. When students are able to safely share their ideas with an audience broader than just our classroom, often they can discover their voice and become even more motivated to learn, communicate and share their ideas effectively with others.

Often we hear negative stories in the mainstream media about the ways young people use the Internet and social media websites. One of the reasons we are participating in some collaborative social media projects this year is to help our students learn through experiences, ways to safely use the Internet to share information and collaborate. Randolph County School System is writing to let you know what we are planning to do, and to obtain your permission for your child to participate.

Planned Activities: We are planning to use several different social media tools to let our students safely share their work and ideas with other students as well as with our school community. (You!) A list of the district recommended websites is located at http://socialmediaguidelines.pbworks.com/District-Recommended-Social-Media-Sites. We encourage you to visit the site to learn more the district's social media guidelines for students, teachers and parents. Projects may be shared privately with other classes over the Internet and with parents, and also may be shared publicly on the Internet. To protect student privacy and ensure safety throughout all projects we will:

1. Only use student first names, if names are used at all, in identifying student work and ideas
2. Not use pictures of individual students, identified by full name
3. Only use GROUP pictures of students that do not identify individuals by name if we share pictures of students working in class.

If you have questions about our projects please contact your child's teacher(s). Teachers will be in contact with you with specific to share links to specific projects as we create them! Please complete, sign and return the bottom of this form to me as soon as possible. Thanks!

_____ YES, my child has my permission to participate in teacher-moderated, Internet-based social media projects this year. My child may share recordings on the Internet and participate in the planned collaborative activities outlined here.

_____ NO, my child does not have permission to participate in these activities.

Date:

Student Name: Student Signature:

Parent Name: Parent Signature:

Sample Permission to Blog Letter

Dear Families:

From now to the end of the year, Mr/Ms _____ class will be taking part in a pilot writing program designed to help them develop their writing and explore their interests by sharing their writing with a real audience. Students will be using personal Weblogs to post their writing to the Internet.

A Weblog, or blog as they are commonly called, is a special type of Web page that can be created and easily updated using a Web browser. Each new entry has its own date stamp. Each entry has a comments section where visitors to the blog may leave comments for the author.

How it Works

Each week Ms. Wenn will teach a writing lesson using the 6-Trait writing model. After the lesson, students will write an entry for their blog. They may choose the topic, but they need to make use of the skills taught in the lesson to help the craft their writing. The emphasis is on the quality, not the quantity of what they write. When students are done polishing their writing, they have it reviewed by a teacher before it is published to the Web.

Students will have two extra computer sessions most weeks to provide them with the time needed to complete their weekly blogging assignment. Students may also work from home. All that is required is an Internet connection and a Web browser. Students are able to save their work as drafts before publishing it to their blog. Directions for working from home will be provided.

Having a real audience is one of the key components to this program. In addition to receiving comments from their classmates, Ms. Wenn's students will receive comments from Ms. Wenn. Parents are also invited to visit the blogs and respond to the writing. Potentially, anyone on the Internet could respond to our blogs, however, it is not likely that the world at large will stumble across them.

Security

This blogging project is designed to minimize risk to your child. The only personally identifying information included in the blog will be their first name. There will be no mention of our school name or our location. Students are allowed to post their interests and opinions, but not their age, email address, photographs of themselves, or other sensitive information.

Assessment

The weekly blog assignments will be part of your child's language arts grade this term. As with other projects they have completed this year, students will receive a scoring rubric that explains the expectations for these assignments. The rubric will include a section for the comments they leave in other students' blogs.

Resources

- Blogs created by fifth grade students in the USA

http://itc.blogs.com/marcos/

- BBC News article about blogging in a school in the UK

http://news.bbc.co.uk/1/hi/magazine/3804773.stm

Permission

Before your child may start posting to their blog, we are asking for you and your child to discuss and sign the following form. Please return the form to Ms. Wenn.

Blogging Terms and Conditions

1. Students using blogs are expected to act safely by keeping personal information out of their posts. You agree to not post or give out your family name, password, user name, email address, home address, school name, city, country or other information that could help someone locate or contact you in person. You may share your interests, ideas and preferences.

2. Students using blogs agree not to share their user name or password with anyone besides their teachers and parents. You agree to never log in as another student.

3. Students using blogs are expected to treat blogspaces as classroom spaces. Speech that is inappropriate for class is not appropriate for your blog. While we encourage you to engage in debate and conversation with other bloggers, we also expect that you will conduct yourself in a manner reflective of a representative of this school.

4. Student blogs are to be a forum for student expression. However, they are first and foremost a tool for learning, and as such will sometimes be constrained by the various requirements and rules of classroom teachers. Students are welcome to post on any school-appropriate subject.

5. Students blogs are to be a vehicle for sharing student writing with real audiences. Most visitors to your blog who leave comments will leave respectful, helpful messages. If you receive a comment that makes you feel uncomfortable or is not respectful, tell your teacher right away. Do not respond to the comment.

6. Students using blogs take good care of the computers by not downloading or installing any software without permission, and not clicking on ads or competitions.

7. Students who do not abide by these terms and conditions may lose their opportunity to take part in this project.

I have read and understood these blogging terms and conditions. I agree to uphold them.

student's signature:_____ date: _____

parent's signature: _____ date: _____

USE OF DIGITAL DEVICES DURING THE ADMINISTRATION OF A SECURE TEST

The following School Test Security Plan shall be enforced at each school in accordance with the Georgia Department of Education Digital Device Policy for the Georgia DRC Milestones End-Of-Grade and End-Of-Course Assessment Guidelines.

A. The possession of a digital device (including but not limited to laptops, smart phones, smart watches, fitness trackers, MP3 players, tablets, cameras, or other communication devices capable of capturing or relaying information) is strictly prohibited during the administration of a secure test. School personnel shall implement a plan to collect all such devices from students before the student enters the testing room. Any digital device that is medically necessary for the health or well-being of the students may be permitted as an exception to this policy if the exception is pre-approved in writing by the Building Test Coordinator or school principal by completion and approval of a Digital Device Exception Request form.

B. If a student is in possession of a digital device within the testing room when participating in Georgia Milestones DRC testing the device will be confiscated, and testing for the student will cease. The digital device shall be subject to search for information directly related to the test being administered if the appropriate administrator determines that there is reasonable suspicion that the device was used to capture, record or share test information or to facilitate cheating on the test. The student also will be dismissed from testing, and the student's test will be invalidated. Violation of this policy may result in suspension or expulsion of the student.

CONSEQUENCES OF POLICIES VIOLATIONS

These combines policies apply to an Randolph County School District community member and refers to all information resources, whether individually controlled, shared, stand-alone, or networked. Disciplinary action, if any, for students, staff, and other users will be consistent with Randolph County School District's policies and procedures.

Where external networks are used, policies governing such use are also applicable and must be adhered to. Violation can cause revocation of access privileges, suspension, or permanent removal or access to Randolph County School District resources, another school's disciplinary action, and/or appropriate legal action, Exact disciplinary measures will be determined on a case-by-case basis. Violations of the laws of the United States or the state of Georgia also may subject the users to criminal prosecution.

Violations of any of these policies—by students, staff, or community members—may result in:

- **Warnings or Restricted Access**
- **Disciplinary Action (up to dismissal or expulsion)**
- **Legal Action for Serious Infractions**
- **Account Suspension or Deletion (for school-sponsored accounts)**

The school Principal, Resource Officer, Director of Technology, Counselor, Disciplinarian, and/or other school personnel will address any violations of said policies. The Randolph County School District will expedite any procedures to eliminate as much of a disruption in the learning process as possible. A tribunal/school hearing will take place within 48 hours (business) of the complete investigation regarding any infraction or violation of policies.

ESTIMATED REPAIR/REPLACEMENT COST OF IT EQUIPMENT

If the Randolph County School District finds that a staff member, student, etc. is responsible for the repair of the device or the replacement of the device, the following information may be used to estimate the individual's amount of responsibility.

Laptop:	Surface Studio Slider	$1700
	Surface Pro 10 w/keyboard	$1500 - $1700
	Surface Pro Workbook 2	$800
	All other laptops	$800
	Charging Cord	$40
Chromebooks	HP 3100 (non-touch)	$240
	HP 31000 (touch)	$320
	Charging Cord	$30
Interactive Display	Clear Touch 75 w/PC+cart	$5000
	Clear Touch 65 w/PC+cart	$4200
	Clear Touch 85 w/PC+cart	$8000
iPad	iPad (standard)	$300
Cases		$25

The above prices are approximate and may fluctuate according to availability and other factors beyond the Randolph County School District's control.

By accepting this agreement I acknowledge that I have read and understand the "Acceptable Use of Computer Technology and Other Related Resources" and I understand my rights and responsibilities regarding the uses of any district owned laptop, desktop, iPad, Chromebook, tablet or other technology device that is assigned to me or device that I may use while employed or enrolled with the Randolph County School District.