ACCEPTABLE USE OF COMPUTER TECHNOLOGY AND RELATED RESOURCES

2024-2025

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. Addition information can be found at https//www.sowegak12.org. The Randolph County School System does not discriminate on 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 technology 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 the 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 in 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 action. 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 of 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. Transmittal 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 damages 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 –

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 action.

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 shall 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 <u>Artificial Intelligence Acceptable Use</u> - 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 that my 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 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 device 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.

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.