Rutherford County Schools

Instructional Technology

RESPONSIBLE MOBILE DEVICE USE POLICY & TECHNOLOGY HANDBOOK

for PARENTS, STUDENTS *and* Staff

Contents

Introduction

The Rutherford County School System's objective is that students and employees benefit from instructional technology resources while remaining within the bounds of safe, legal and responsible use. Accordingly, RCS establishes this Mobile Device Responsible Use Policy and Technology Handbook to govern student and staff use of school district instructional resources. This policy applies regardless of whether such use occurs on or off school district property, and it applies to all school district instructional 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.

About Mobile Devices

The Dell Latitude 3180s are designed to enrich education and empower students. For our district this choice in mobile device is a cost-effective learning solution built with the best-in-class durability to withstand every school day. It is built with a liquid resistant keyboard and click pad along with rubberized base trim to absorb shock from bumps.

Who will Participate in $2_{to}1$

Middle school classrooms in Rutherford County School System grades 6, 7 and 8 will be provided a learning device to use in the classroom at 2 students to 1 device ratio beginning in the 2018/2019 school year. RCS strongly believes this initiative is a vital component in preparing students to be college and career ready. Holloway High School, Daniel McKee Alternative School and Smyrna West Alternative School will be served as 2:1 schools starting in the 2018/2019 school year.

I have my own device.

You may use your own device. However, RCS does not support a student owned device. Teachers may be using programs and have lesson plans that may not work on devices not supported by the district. Contact your principal if you have any questions.

General Expectations for Use of School Technological Resources

1. District technological resources are provided for school-appropriate purposes only. Acceptable uses of such technological resources are limited to responsible, efficient and legal activities that support learning and teaching.
2. Student and staff use of school district technological resources for political purposes or for commercial gain or profit is prohibited.
3. Student and staff personal use of school district technological resources for social media, amusement or entertainment during the school day is also prohibited. Waivers may be allowed on a case-by-case basis for educational purposes that require the use of social media. Waivers shall be obtained from the school principal or designee.
4. Students and staff must comply with all applicable laws, including those relating to copyrights and trademarks, confidential information, and public records. Any use that violates state or federal law is strictly prohibited. Plagiarism of Internet resources will be treated in the same manner as any other incidents of plagiarism.

5. 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. All users must comply with RCS policies and procedures.

6. The use of anonymous proxies to circumvent content filtering is prohibited.

7. Users may not install or use any Internet-based file-sharing program designed to facilitate sharing of copyrighted material.

8. Users of technological resources may not send electronic communications fraudulently (i.e., by misrepresenting the identity of the sender).

9. Users must respect the privacy of others. When using e-mail, chat rooms, blogs or other forms of electronic communication, students/staff must not reveal personal identifying information (of self or others), or information that is private or confidential, such as the home address or telephone number, credit or checking account information or social security number of themselves or fellow students/staff. Users also may not forward or post personal communications without the author's prior consent.

10. 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.

11. Users may not create or introduce games, network communications programs or any foreign program or software onto any school district computer, electronic device or network without the expressed written permission of the technology director or designee.

12. Users are prohibited from engaging in unauthorized or unlawful activities, such as "hacking" or using the computer network to gain or attempt to gain unauthorized or unlawful access to other computers, computer systems or accounts.

13. Users are prohibited from using another individual's ID or password for any technological resource.

14. Users may not read, alter, change, block, execute or delete files or communications belonging to another user without the owner's express prior permission.

15. If a user identifies a security problem on a technological resource, s/he must immediately notify a system administrator. Users must not demonstrate the problem to other users. Any user identified as a security risk will be denied access.

16. 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.

17. 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, as well as content.

Handling, Care and Use by Students

- Students who are issued district owned and maintained devices must also follow these guidelines:
    - Keep the device secure and damage free.
    - Do not loan out the device, charger or cords.
    - Do not leave the device in a vehicle.
    - Do not eat or drink while using the device or have food or drinks in close proximity to the device.
    - Do not place the device on the floor or on a sitting area such as a chair or couch.
    - Do not leave the device near table or desk edges.
    - Do not stack objects on top of the device.
    - Do not leave the device outside.
- Students are responsible for all media, Internet usage, downloads, file creation, file deletion, file sharing, file storage, and other actions that involve all software or applications accessed via your assigned device. **Do not allow other users to use the device assigned to you.**
- Student devices are only for creation of, storage of, access to, and consumption of school-appropriate content. Do not access, store, create, consume, or share unauthorized or inappropriate content with your device.
- Students are responsible for ensuring their assigned device logs on to the school district's network daily to receive necessary updates that are critical to keeping the device safe and operational.
- Students are responsible for ensuring nothing is ever connected to, or inserted into, any of the ports and/or connectors of the device that are not intended for that particular port or connector.
- Students are responsible for ensuring the device is never exposed to liquids or other foreign substances, including drinks, paint, ink, glue, cleaners, polishes, or any type of health/beauty aid (lotion, nail polish, perfume, soap, shampoo, etc.).
- Students are responsible for ensuring the surface of the device is not altered or defaced. Students cannot decorate their assigned device or remove labels, stickers, or tags from the device that are affixed by school district personnel.
- Make sure that only school district personnel troubleshoot, diagnose, or repair your assigned device.

Security, Storage and Transport

- Keep the device powered on (to ensure updates) and in storage site when not in use.
- Do not hold, lift, or suspend the device in the air solely by the screen/display.
- Transport the device with a two-hand grip always.
- Make sure to power the device completely off before inserting it into a protective carrying case if it will be stored there for a duration of longer than 5 minutes.
- Relocate a device that is powered on, opened up, and in use for class to a secure location to be monitored by a staff member if leaving the classroom at school. Do not leave it on a small or unstable desk in a classroom if you are leaving the room, even if only for a moment.
- Keep your device secure. Students are responsible for their assigned device at all times. Students should return their assigned device to the designated storage at the end of the school day. Devices should not be left out in a classroom for overnight storage even if the classroom is to be locked.
- Students are responsible for ensuring that their assigned device is not shared or switched, its power charger, and/or other accessories with other users.

Privacy

No right of privacy recognized in the use of technological resources owned by RCS. Users should not assume that files or communications accessed, downloaded, created or transmitted using school district technological resources or stored on services or hard drives of individual computers will be private. School district administrators or individuals designated by the superintendent may review files, monitor all communication and intercept e-mail messages to maintain system integrity and to ensure compliance with board policy and applicable laws and regulations. School district personnel shall monitor on-line activities of individuals who access the Internet via a school-owned computer. Under certain circumstances, RCS may be required to disclose such electronic information to law enforcement or other third parties pursuant to court orders.

Parental Consent

The Rutherford County School System 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 parent 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 e-mail communication and Internet activity by school personnel.

Microsoft Account

Through an RCS student login, the district provides students with a district owned and managed account to access Microsoft Apps with Office 365. Microsoft provides access to specific Microsoft products to school districts on an a-la-carte basis. RCS chooses which app services students have access to and manages the secure accounts in a "Walled Garden". Services that students have access to include, but are not limited to, Word, Excel, Forms, PowerPoint and Calendar.

Office 365 email

As a part of the district's Office 365 account, students in grades 3 through 12 have access to a Microsoft email account. The purpose of this service is to allow students to collaborate and communicate with each other and their teachers. RCS will use the "Walled Garden" approach, meaning students do not have the ability to send email to or otherwise communicate with anyone outside of the school district. All emails are archived and may be reviewed at any time by an administrator. Students do not have entitlement to privacy with their school issued email account.

Other School Issued Accounts

To provide access to appropriate online resources and services, their teachers or schools may issue students accounts. Because new technologies are being developed every day, students may gain or lose access to different services or resources during the school year. It is within the discretion of the Director of Schools or his/her approved designee to approve accounts to be utilized. Teachers who assign accounts to utilize services not on this list will notify parents directly. All services and resources will be vetted for appropriateness of content and compliance with Federal CIPA and COPPA privacy regulations. Educational software and web based educational tools do collect and store the students' information as to assess their progress. It is our duty to inform each parent that personal information is collected for education and assessment purposes.

Digital Leadership: Social Media Guidelines

- Be aware of what you post online. Social media venues are very public. What you contribute leaves a digital footprint for all to see. Do not post anything you wouldn't want friends, enemies, parents, teachers, or a future employer to see.
- Follow the school's code of conduct when writing online.
- Be safe online. Never give out personal information, including, but not limited to, last names, phone numbers, addresses, exact birthdates, and pictures. Do not share your password with anyone outside of your teachers and parents.
- Linking to other websites 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.
- Do your own work! Do not use other people's intellectual property without their permission. Be aware that it is a violation of copyright law to copy and paste other's thoughts. It is good practice to hyperlink to your sources.
- Be aware that pictures may also be protected under copyright laws. Verify you have permission to use the image or that it is able to be used under Creative Commons attribution.
- How you represent yourself online is an extension of yourself. Do not misrepresent yourself by using someone else's identity.
- Blog and wiki posts should be well written. Follow writing conventions including proper grammar, capitalization, and punctuation. If you edit someone else's work, be sure it is in the spirit of improving the writing.
- If you run across inappropriate material that makes you feel uncomfortable, or is not respectful, tell a parent or teacher right away.
- 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.

File Storage

- Every student is provided Microsoft OneDrive storage for school-related files and content.
- Flash drives, SD Cards, etc. formatted as storage devices can be used on RCS Devices.
- Note: Any time a device requires repair or maintenance, all data and documents stored locally on the device will be lost.

Content Filtering and Restricted Material on the Internet

RCS employs a third-party filtering application on all district computers that is updated regularly. These updates are pushed to student devices each time they are logged on to the district's network. The content filter, as configured by the district and as operates on the device in possession of a student who is using the device will restrict inadvertent access to unapproved content online and deter attempts to deliberately access unapproved content online. This does not absolve the user from attempting to access unauthorized or inappropriate sites on the Internet. Attempts to disable, reconfigure, or circumvent the content filter is a violation of the aforementioned usage policies and can result in administrative referral for disciplinary consequences or restrictions of a student's technology use privileges.

Because of the nature of the Internet, no content filter is capable of preventing all access to all online content that is not school-related. Although the content filter will provide a degree of protection to the user and the device, the user assumes responsibility for not accessing content that is not school-related, whether blocked

by the filter at that particular time or not. RCS recognizes that it is impossible to predict with certainty what information on the Internet students may access or obtain. Never the less school district personnel shall take reasonable precautions to prevent students from accessing material and information that is obscene, pornographic or otherwise harmful to minors, including violence, nudity, or graphic language that does not serve a legitimate pedagogical purpose. RCS shall ensure that technology protection measures are used and are disabled or minimized only when permitted by law and board policy. RCS is not responsible for the content accessed by users who connect to the Internet via their personal mobile telephone technology (e.g., 3G, 4G service). Any access of unapproved content online, whether through a district-owned device, personal cell phone, or any other personal electronic device, while at school is a violation of this usage policy.

Reporting Damage to Device

By taking possession of an assigned device, the user (student or staff) agrees to assume full responsibility for the safety, security, and care of the borrowed property.

- In the case of loss or theft occurring at school, the assigned user must report the incident to school administration of the appropriate building within one school day of the occurrence.
- In the case of loss or theft occurring away from school, the borrower must report the incident tothe law enforcement officials of jurisdiction within 24 hours of the occurrence and then provide documentation of the police report to school administrators.
- Failing to report loss or theft in the manner described here will result in the missing property being categorized as lost rather than stolen and the student/parent/guardian will assume full responsibility for the loss of the device and the corresponding financial obligation for the replacement costs of the lost property.
- In the case of damage to a assigned device, you must report the potentially damaging incident to school administrators of the appropriate building within one school day of the occurrence.
- Failing to report damage or potentially damaging incidents in the timely manner described above will result in the user assuming responsibility of necessary repair costs for the damaged property.

Repair Costs

- Repairs will be made to an assigned device if the nature of the damage makes the device inoperable or leaves the device in a state where the damage is likely to increase after redistribution resulting in need for repair for a future user.

Repair	Cost
Broken Screen	$67.99
Charger	$51.44
Broken or Missing Keys (Keyboard replacement)	$16.99
Damage to USB/HDMI/SD ports (System Board replacement)	$178.91
Damage to Audio Port	$9.99
Battery Replacement	$28.99

Although the information in this price list is presented in good faith and believed to be correct at the time of publishing, RCS makes no representations or warranties as to the completeness or accuracy of the information. RCS has no liability for any errors or omissions in the price listing. (last updated 10/18/18)

Replacement Costs

- A student/parent/guardian is responsible for cost of replacement of a lost mobile device if the loss of the borrowed property is not reported according to the "Reporting Loss/Damage" section or the borrowed device is lost as the result of handling, storing, or using in a manner not in compliance with the "Security, Storage, and Transport" guidelines.
- The replacement cost of a lost device is based on the cost of a replacement device.
- A student/parent/guardian is fully responsible for the replacement cost of any device accessories lost while in their possession.
- Replacement costs of device accessories are based on the price for which RCS purchases replacement accessories from 3rd party vendors.

Parent/Guardian Initiated Accommodations

It is the belief of RCS that every student should be granted equal access to the resources provided by the school district for learning. It is not the district's recommendation that a student be restricted access to any learning resource that is granted to all other students. If circumstances outside of school call for a student to have limited or restricted access to district-provided resources, a written request by the student's parent/guardian, in collaboration with a school administrator, must be placed on file with the specific school from which the parent/guardian is requesting the special accommodation. If the request is initiated by parent/guardian, then approved by a school administrator, and placed on file with the school's technology department, a student may be granted "as needed only" or "by teacher request only" access to their device, rather than having it issued into the student's possession.

Administrator-Initiated Accommodations

Noncompliance with the expectations of the *Responsible Mobile Device Use Policy* can result in the loss of privilege with, or restricted access to, district-provided technology as a consequence for misuse or a safety measure for a particular student. If this is the case, a school administrator will collaborate with the student and parent/guardian to make arrangements that may deny or restrict access to the resource in question. The use of RCS technology is a privilege rather than a right and can, therefore, be taken away from a user who has displayed behavior, or a pattern of behavior, that is considered by an administrator to be potentially unsafe or unhealthy for the user, other students, staff, the technology itself, or the learning environment.

Repossession

If you do not fully comply with all terms of the *Responsible Mobile Device Use Policy*, including the timely return of the property, the RCS shall be entitled to come to your place of residence, or other location of the device, to take possession of the property.

Appropriation

Your failure to timely return the property and/or the continued RCS property for non-school purposes without the District's consent may be considered unlawful appropriation of the District's property.

Disclaimer

The RCS makes no warranties of any kind, whether express or implied, for the service it is providing. RCS will not be responsible for any damages suffered by any user. Such damages include, but are not limited to, loss of data resulting from

delays, non-deliveries or service interruptions, whether caused by the school district's or the user's negligence, errors or

omissions, physical or emotional harm resulting from use of device. Use of any information obtained via the Internet is at the user's own risk. The school district specifically disclaims any responsibility for the accuracy or quality of information obtained through its Internet services.

Portions Modified/Quoted from the Lebanon Special School District, Lebanon, TN, Mooresville Graded School District, Mooresville, NC and North Kansas City Schools, Kansas City, MO. Legal References: U.S. Const. Amend. I; Children's Internet Protection Act, 47 U.S.C. 254(h)(5); Electronic Communications Privacy Act, 18 U.S.C. 2510-2522; Family Educational Rights and Privacy Act, 20 U.S.C. 1232g; 17 U.S.C. 101 et. seq.; 20 U.S.C. 6777; G.S. 115C-325(e); RCS Board Policies; and Student Handbooks

RCS reserves the right to update this Responsible Mobile Device Use Policy at any time deemed necessary. For the most up-to-date RMDUP, please visit our website https://www.rcschools.net/