



Rockwood Area School District Chromebook Program

KINDERGARTEN -12TH GRADE
2021-22

One-to-One Technology Integration

The Rockwood Area School District is committed to preparing and empowering its students with 21st century skills by issuing a Chromebook to all students in grades K-12. This handbook is intended to outline the District's expectations of proper handling of Chromebooks, Students' Responsibilities and Care for their Chromebook, Student/parent User Agreement, and Acceptable User Agreement.

WHAT IS A CHROMEBOOK?

Chromebooks are digital laptop devices that run a chrome operating system by Google. They are a newer type of computer that uses technology with a single google account. Essentially, they are web browsers that connect to the internet. Chromebooks automatically update and run in the cloud or remote web servers so users do not need to worry about hard drive storage.

Handling of Chromebooks

Receiving/Returning your Chromebook

1. Parent/Guardian Orientation – All parents/guardians are required to sign the user agreement, GSuite agreement, and internet usage agreement located in the back of the student handbook.
2. Student Distribution – All students are required to sign the user agreement prior to being issued a Chromebook.
3. New Students – All new students will be able to pick up their Chromebook in the Technology Office after enrolling. Parents/Guardians will also be required to complete the orientation and sign the user agreement.
4. Students will be issued a Chromebook for a four-year period. They do not need to be collected at the end of the school year and will be updated automatically when they return to school. At the end of the four-year period, students will be permitted to keep their Chromebook.

Chromebook Loan Agreement

A Chromebook and power supply are being lent to the student for a period of four years. The Chromebook remains the property of the Rockwood Area School District during this time and is being lent to the student for educational purposes. The student may not deface or destroy this property in any way. The equipment is

for the use of the student only; family and friends should not use equipment. Inappropriate use of the device may result in loss of Chromebook privileges. If the student withdraws from RASD prior to the end of the four-year period, the device shall be returned.

The student may not make, or allow others to make, any attempts to add, delete, access, or modify District owned information on any Chromebook. The RASD network is provided for the academic use of all students and staff.

Equipment identification stickers have been placed on all Chromebooks and power cords. The labels shall not be removed or modified. If they become damaged or missing, contact the technology department immediately. ***Additional stickers, labels, markings of any kind are not to be added to the device.***

Each student currently has a student Gmail account which includes the student's id number@rockwoodschoools.org. This email is for appropriate academic communication only and is for use only within the school district.

No one should have any expectation of privacy or confidentiality with regard to any use of the Chromebook issued by the District. During school hours, without prior notice of consent, the District may access, supervise, view, monitor and record student use of Chromebooks at any time for any reason related to the operation of the District. Chromebook browsing history is always logged.

Monitoring Software – School administrators may use monitoring software that allows them to view screens and activity on student Chromebooks at any time during school hours.

Files downloaded onto Chromebooks become the property of Rockwood Area School District, which may include images, documents, files, and/or apps.

Responsibilities

Student Responsibilities:

The Chromebook is a privilege and can be a valuable educational tool. It is to be used for education purposes only. In order to have this privilege, you must be willing to accept the following responsibilities:

- ✓ When using the Chromebook, the student will follow the policies of Rockwood Area School District, including the Internet Acceptable Use Policy, and agrees to abide by all local, state, and federal laws.
- ✓ I will treat the Chromebook with care by not dropping it, getting it wet, leaving it in the car, outdoors, unsecured, or in a place it may become damaged or stolen.
- ✓ I will not lend the Chromebook to anyone.
- ✓ I will not remove ANY District-owned programs or files.
- ✓ I will charge my Chromebook each night so it has a full charge at the start of every school day.
- ✓ I understand if I do not charge it or forget it at home, I am still responsible for getting my course work completed.
- ✓ I agree that email (or any electronic communication) should be used for only appropriate, legitimate and responsible communication.
- ✓ I will not attempt to repair the Chromebook. If it is not working properly, I will create a HELP ticket within the IT department.
- ✓ I will bring the Chromebook to IT support staff if it needs repaired. If the device needs repaired the student's record will be checked, a loaner may be checked out if the student is eligible and a device is available. Appropriate fees will be charged.

Parent/Guardian Responsibilities:

A Chromebook is being issued to your son/daughter as an academic tool to enhance their overall educational experience.

- ✓ I will not attempt to repair the Chromebook, nor will I attempt to clean it with anything other than a dry cloth.
- ✓ I will make a report to the technology department with any problems associated with the device or software.
- ✓ I will not delete any District software.
- ✓ I will make sure my child charges the device each night.
- ✓ I will return the Chromebook when it is requested by the school or upon my child's withdrawal from the district.

- ✓ I will support my child by supervising their internet usage and email while they are at home.

For parent safety resources and tips visit www.google.com/safetycenter

Acceptable Use of Internet, Computers, and Network Resources (also found on p. 33 of the student handbook)

The Board supports the use of computers, Internet and other network resources in the district's instructional and operational programs in order to facilitate learning, teaching and daily operations through interpersonal communications and access to information, research and collaboration. The district provides students, staff and other authorized individuals with access to the district's computers, electronic communication systems and network, which includes Internet access, whether wired or wireless, or by another means. For instructional purposes, the use of network facilities shall be consistent with the curriculum adopted by the district as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.

Child pornography – under federal law, is any visual depiction, including any photogram, film, video, picture, or computer or computer generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct.

Harmful to minors – under federal law, is any picture, image, graphic image file or other visual depiction.

Obscene – any material or performance, if:

1. The average person applying contemporary community standards would find that the subject matter taken as a whole appeals to the prurient interest;
2. The subject matter depicts or describes in a patently offensive way, sexual conduct described in the law to be obscene; and
3. The subject matter, taken as a whole lacks serious literary, artistic, political, educational or scientific value.

Technology protection measure – a specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography or harmful to minors.

The availability of access to electronic information does not imply endorsement by the district of the content, nor does the district guarantee the accuracy of information received. The district shall not be responsible for any information that may be lost, damaged or unavailable when using the network or any information that is retrieved via the internet.

The district shall not be responsible for any unauthorized charges or fees resulting from access to the Internet or other network resources.

The Board declares that computer and network use is a privilege, not a right. The district's computer and network resources are the property of the district. Users shall have no expectation of privacy in anything they create, store, send, receive or display on or over the district's Internet, computers or network resources, including personal files or any use of the district's Internet, computers or network access and use; monitor file server space utilization by district users; or deny access to prevent unauthorized, inappropriate or appropriate illegal activity and may revoke access privileges and/or administer appropriate disciplinary action. The district shall cooperate to the extent legally required with the ISP, local, state and federal officials in any investigation concerning or related to the district's Internet, computers and network resources.

The Board requires all users to fully comply with this policy and to immediately report any violations or suspicious activities to the Superintendent or designee.

The Board establishes the following materials, in addition to those stated in law and defined in this policy, that are inappropriate for access by minors:

1. Defamatory.
2. Lewd, vulgar, or profane.
3. Threatening.
4. Harassing or discriminatory.
5. Bullying.
6. Terroristic.

The district reserves the right to restrict access to any Internet sites or functions it deems inappropriate through established Board policy, or the use of software and/or online server blocking. Specifically, the district operates and enforces a technology protection measure(s) that blocks or filters access to inappropriate matter by minors on its computers used and accessible to adults and students. The technology protection measure shall be enforced during the use of computers with Internet access.

Upon request by students or staff, the Superintendent or designee shall expedite a review and may authorize the disabling of internet blocking/filtering software to enable access to material that is blocked through technology protection measures but is not prohibited by this policy.

Upon request by students or staff, building administrators may authorize the temporary disabling of Internet blocking/filtering software to enable access for bona fide research or for other lawful purposes. Written permission from the parent/guardian is required prior to disabling Internet blocking/filtering software for a student's use. If a request for temporary disabling of Internet blocking/filtering software is denied, the requesting student or staff member may appeal the denial to the Superintendent or designee for expedited review.

The district shall make every effort to ensure that this resource is used responsibly by students and staff.

Users of district networks or district-owned equipment shall, prior to being given access or being issued equipment, sign user agreements acknowledging awareness of the provisions of this policy, and awareness that the district uses monitoring systems to monitor and detect inappropriate private use and tracking systems to track and recover lost or stolen equipment.

Student user agreements shall also be signed by a parent/guardian. Students will be educated on network etiquette and other appropriate online behavior, including:

1. Interaction with other individuals on social networking web sites and in chat rooms.
2. Cyber-bullying awareness and response.

Network accounts shall be used only by the authorized owner of the account for its approved purpose. Network users shall respect the privacy of other users on the system.

Safety

It is the district's goal to protect users of the network from harassment and unwanted or unsolicited electronic communications. Any network user who receives threatening or unwelcome electronic communications or inadvertently visits or accesses an inappropriate site shall report such immediately to a teacher or administrator. Network users shall not reveal personal information to other users on the network, including chat rooms, e-mail, social networking web sites, etc...Internet safety measures shall effectively address the following:

1. Control of access by minors to inappropriate matters on the internet and world wide web.
2. Safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications.
3. Prevention of unauthorized online access by minors, including "hacking" and other unlawful activities.
4. Unauthorized disclosure, use, and dissemination of personal information regarding minors.
5. Restrict of minors' access to material harmful to them.

Prohibitions

Users are expected to act in a responsible, ethical and legal manner in accordance with district policy, accepted rules of network etiquette, and federal and state law. Specifically, the following uses are prohibited:

1. Facilitating illegal activity.
2. Commercial or for-profit purposes.
3. Non-work or non-school related work.
4. Product advertisement or political lobbying.
5. Bully/Cyber-bullying.
6. Hate mail, discriminatory remarks, and offensive or inflammatory communication.
7. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.
8. Accessing, sending, receiving, transferring, viewing, sharing or downloading obscene, pornographic, lewd, or otherwise illegal materials, or images or photographs.
9. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with Board policy.

10. Inappropriate language or profanity. Transmission of material likely to be offensive or objectionable to recipients.
11. Intentional obtaining or modifying of files, passwords, and data belonging to other users.
12. Impersonation of another user, anonymity, and pseudonyms.
13. Fraudulent copying, communications, or modification of materials in violation of copyright laws.
14. Loading or using of unauthorized games, programs, files or other electronic media.
15. Disruption of the work of other users.
16. Destruction, modification, abuse or unauthorized access to network hardware, software, and files.
17. Accessing the internet, district computers or other network resources without authorization.
18. Disabling or bypassing the internet blocking/filtering software without authorization.
19. Accessing, sending, receiving, transferring, viewing, sharing or downloading confidential information without authorization.

Security

System security is to protect the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or district files. To protect the integrity of the system, these guidelines shall be followed:

1. Employees and students shall not reveal their passwords to another individual.
2. Users are not to use a computer that has been logged in under another student's or employee's name.
3. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.

Consequences for Inappropriate Use

The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts. Illegal use of the network; intentional deletion or damage to files or data belonging to others; copyright violations; and theft of services shall be reported to the appropriate legal authorities for possible prosecution. General rules for behavior and

communications apply when using the Internet, in addition to the stipulations for this policy.

Vandalism shall result in loss of access privileges, disciplinary action, and/or legal proceedings. Vandalism is defined as any malicious attempt to harm or destroy data of another user, Internet or other network; this includes but is not limited to uploading or creating computer viruses.

Failure to comply with this policy or inappropriate use of the Internet, district network or computers shall result in usage restrictions, loss of access privileges, disciplinary action, and/or legal proceedings.

Incident Assessment Chart

Incident	Action (s) Necessary	Cost
<p>1st Offense Accidental Damage of Chromebook, Adapter, or Power Cord</p>	<p>The student makes a report to the Principal or IT Department, who will record the incident.</p> <p>The device is returned to the IT Department and a replacement device may be issued.</p> <p>Parents are notified.</p>	<p>\$25.00</p>
<p>2nd Offense Accidental Damage</p>	<p>The student makes a report immediately to the Principal or IT Department, who will record the incident.</p> <p>The device is returned to the IT Department so a new or spare device may be issued.</p> <p>Some loss of privileges of using the Chromebook may occur such as:</p> <p><i>Limiting participation in the Chromebook program, or the student may not be able to take the device home.</i></p> <p>Parents are notified.</p>	<p>\$25.00 -\$75.00</p> <p>*Upon review of the damage & nature of the incident.</p>
<p>Intentional Damage</p>	<p>Upon notification of an intentional incident involving damage or abuse, the device must be returned to the IT Department.</p> <p>The student loses his/her privileges of using the Chromebook.</p>	<p>Up to the repair or replacement cost.</p>

	<p>*Refer to RASD student code of conduct and appropriate disciplinary response according to the type of infraction.</p> <p>Parents are notified.</p>	
Loss/Theft	The student/parent makes a report immediately to the administration. Administration or IT Department and investigation is completed.	Replacement cost
Denied Claim by Insurance	<p>If the student's Chromebook damage claim is denied by the District's insurance company.</p> <p>Below are the circumstances why a claim can be denied.</p> <p>Damage caused by non - accidental</p> <p>If the student does not give clarification on the details provided about how the device was damaged</p> <p><u>Actions taken:</u></p> <p>Upon notification of an intentional incident involving damage or abuse, the device must be returned to the IT Department.</p> <p>The student may lose his/her privileges of using the Chromebook.</p> <p>*Refer to RASD student code of conduct and appropriate disciplinary response according to the type of infraction.</p> <p>Parents are notified.</p>	Up to the repair or replacement cost.

Chromebook User Agreement Signature Page

Student Last Name _____	First Name _____	MI _____
Grade _____	Student ID # _____	
Parent/Guardian Name _____		

Student Agreement for Chromebook Use:	Parent/Guardian Agreement:
<p>I, _____ agree to the following:</p> <ul style="list-style-type: none"> ✓ While using the Chromebook, I will follow the policies of the Rockwood Area School District, including the Internet Acceptable Use Policy, and I will abide by all local, state, and federal laws. ✓ I will treat the Chromebook with care by not dropping it, getting it wet, leaving it in the car, outdoors, unsecured, or in a place it may become damaged or stolen. ✓ I will not lend the Chromebook to anyone. ✓ I will not remove ANY District-owned programs or files. ✓ I will charge my Chromebook each night so that it has a full charge at the start of every school day. ✓ I understand if I do not charge it or forget it at home, I am still responsible for getting my course work completed. ✓ I agree that email (or any electronic communication) should be used for only appropriate, legitimate and responsible communication. ✓ I will not attempt to repair the Chromebook. If it is not working properly, I will create a HELP ticket within the IT department. ✓ I will bring the Chromebook to IT support staff if it needs repaired. If the device needs repaired the students record will be checked, a replacement may be provided if the student is eligible and once the appropriate fees are paid by the student to the District account. 	<p>I, _____ agree to the following:</p> <ul style="list-style-type: none"> ✓ I will not attempt to repair the Chromebook, nor will I attempt to clean it with anything other than a dry cloth. ✓ I will make a report to the technology department with any problems associated with the device or software. ✓ I will not delete any District software. ✓ I will make sure my child charges the device each night. ✓ I will return the Chromebook when it is requested by the school or upon my child's withdrawal from the district. ✓ I will support my child by supervising their internet usage and email while they are at home.
<p>Student Signature _____</p>	<p>Parent Signature _____</p>
<p>Date _____</p>	<p>Date _____</p>