Technology

ACCEPTABLE USE POLICY AND GUIDELINES

Introduction

This document formalizes the policy for users of the Richmond Consolidated School (RCS) Network resources. All users, including but not limited to students, teachers, administrators, staff, guests and educational organizations are covered by this policy and are expected to be familiar with its provisions.

User Responsibilities

It is the responsibility of any person using the RCS Network resources to read, understand, and to follow these guidelines. In addition, users are expected to exercise reasonable judgment in interpreting these guidelines and in making decisions about the appropriate use of the RCS Network resources. Any person with questions regarding the application or meaning of these guidelines should seek clarification from the RCS Network Administrator. Use of the RCS Network resources shall constitute acceptance of the terms of these guidelines. It is the responsibility of any person using the RCS devices such as teacher laptops and student Chromebooks to read, sign and submit the RCS Acceptable Use policy online document.

RCS Network Administrator Responsibilities

It is the responsibility of the person who has been designated as the RCS Network Administrator to ensure that only educators and students in his/her school are registered users of the RCS Network. The Administrator is responsible for making certain that the educators and students within the school understand and abide by the Acceptable and Unacceptable Uses as stated in this document (Paragraph 3). If the RCS Network Administrator has reason to believe that a user (educator or student) is misusing the system, the Administrator has the right to access the user's account in order to review the use of the RCS Network tools by the user. It is also the responsibility of the Administrator to report any misuse of the system to the Principal.

RCS Educator Responsibilities

It is the responsibility of educators who are using the RCS Network resources with students to teach students about safe and responsible use of the Internet and the RCS Network. Educators are responsible for monitoring students' use of these resources, and to intervene if students are using them inappropriately. Educators should make sure that students understand and abide by the Acceptable and Unacceptable Uses as stated in this document (Paragraph 3). If an educator has reason to believe that a student is misusing the system, he or she has the right to request that the RCS Network Administrator review the use of the RCS Network tools by the student. It is also the responsibility of the teacher to report any misuse of the system to his/her RCS Network Administrator or directly to the Principal.

RCS Network Student Responsibilities

It is the responsibility of students who are using the RCS Network resources to learn about safe and responsible use of the Internet and RCS Network. They are responsible to use these resources responsibly and appropriately. They must abide by the Acceptable and Unacceptable Uses as stated in this document (Paragraph 4). If a student is misusing the system, RCS educators or the RCS Network Administrator must report it to the Principal and/or the RCS Network Administrator who have the right to discontinue his/her use of the system.

Technologies Covered

RCS may provide the privilege of Internet access, desktop computers, mobile computers or devices, iPods, iPads, cell phones, videoconferencing capabilities, online collaboration capabilities, message boards, email and more. This Acceptable Use Policy applies to both school owned and privately owned devices accessing the RCS network, the RCS Internet connection, and/or private networks/Internet connections while on school property. The policies outlined in this document cover *all* available technologies now and into the future, not just those specifically listed or currently available.

Technology Educational Technology Tools (EdTech) being used this year at Richmond Consolidated School

This year students will be using a variety of EdTech tools (websites/apps) during core class time as well as specialist classes.

We strive to review these websites and apps regularly to make sure they are following the Family Educational Rights and Privacy Act (FERPA), which is a federal law enacted in 1974 that protects the privacy of student education records and Children's Online Privacy Protection Act (COPPA) which requires that the federal trade commission to issue and enforce regulations concerning children's online privacy. We have adopted a process for reviewing these apps and websites and we now belong to the Student Data For Privacy Consortium (SDPC) along with other schools in Massachusetts. These schools all work together to stay updated on student data privacy laws and best practices.

If you have any questions regarding the websites/apps that students are using, please contact the school.

Acceptable and Unacceptable Uses

The resources available to the RCS Network users are to be used for educational purposes. All RCS Network users are responsible for all activity on the RCS Network. Users should not use the RCS Network to store any files that are not educational.

It is acceptable for users to:

• Use school technologies for school-related activities.
• Follow the same guidelines for respectful, responsible behavior online that is expected offline.
• Treat school resources carefully, and alert staff if there is any problem with their operation.
• Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
• Alert a teacher or other staff member if observing any threatening, inappropriate, or harmful content (images, messages, posts) online.

• Use school technologies at appropriate times, in approved places, for educational pursuits.
• Cite sources when using online sites and resources for research.
• Recognize that use of school technologies is a privilege and treat it as such.
• Be cautious to protect their own safety and the safety of others.
• Help to protect the security of school resources.

It is unacceptable for users to use these resources for:

• Furthering any political or religious purpose.
• Engaging in any personal, commercial or fundraising purpose.
• Sending threatening or harassing messages in accordance with the RCS Bully Prevention Plan.
• Gaining unauthorized access to computer or telecommunications networks.
• Interfering with the operations of technology resources, including placing a computer virus on any computer system, including the RCS Network system.
• Accessing or sharing sexually explicit, obscene, or otherwise inappropriate materials.
• Intercepting communications intended for other persons.
• Attempting to gain unauthorized access to the RCS Network system.
• Logging in through another person's account or attempting to access another user's password or files.
• Sending defamatory or libelous material concerning a person or group of people.
• Furthering any illegal act, including infringing on any intellectual property rights.
• Downloading, uploading, or distributing any files, software, or other material that is not specifically related to an educational project.
• Downloading, uploading, or distributing any files, software, or other material in violation of federal copyright laws.

Mobile phones with cameras and screens create a new set of privacy issues for the school as images of people can be taken without their knowledge, images can be saved and then sent to other people, and it is possible to send these images to the Internet. This creates the potential for gross invasion of privacy in areas around the school such as rest rooms and on field trips. In cases where there are gross invasions of privacy or where student images are used without permission (i.e., sent to another person or posted on the Internet) there will be serious consequences. In some cases, students could be suspended from school and in extreme circumstances they could be expelled from school.

This is not intended to be an exhaustive list. The administration reserves the right to hold users accountable for any improper use. Users should use their own good judgment when using school technologies.

As with any other form of communication, these systems may not be used to transmit or store messages or other data that are inappropriate under existing RCS Network, district or MA DOE policies, such as those prohibiting bullying and sexual harassment. Users may not create, send, or store messages or other data that are considered offensive, contain sexually explicit material, or otherwise offensively address the age, race, ethnicity, gender, sexual orientation, religious or political beliefs, national origin, or disability of a person or a group of people. Users also may not create, send, or store messages pertaining to dangerous devices such as weaponry or explosive devices. Users should take all reasonable precautions against receiving or downloading messages, images, or other data of this sort.

No Expectation of Privacy

The RCS Network resources are the property of the Richmond Consolidated School and are to be used in conformance with these guidelines. The RCS Principal and Network Administrator retain the right to inspect any user's data and communications. The RCS Principal and Network Administrator also have the right to give permission to the teachers, the school administrators, and the parents of any student to review the use of the RCS Network tools by a student who they think may be misusing the system. Users are advised that messages in discussion forums, including deleted messages, are regularly archived and can be retrieved. In addition, an Internet firewall automatically checks all data moving between the local area network and the Internet and logs the sending and receiving destinations. Use of the RCS Network resources constitutes consent for the RCS Network Administrator to monitor and/or inspect any files that users create, any messages they post or receive, and any websites they access. Any email communication between staff or staff and parents regarding students could be considered part of a student's record. This must be preserved in accordance with student record laws.

Passwords

Administrators and teachers shall be given a private login and password for access to teacher related resources on the RCS Network. This username and password is to be used to access the RCS Network and any resources that reside within the RCS Network that require password access. The users must take precautions to maintain the secrecy of their password so that other users will not be able to utilize that password for malicious purposes. If a user suspects that someone has discovered the user's password, the user should change the password immediately.

Students will have access only to student-related resources on the RCS Network. If any user (student, teacher, or administrator) suspects that someone has discovered a teacher or administrator password, the user must report such discovery to the RCS Network Administrator or the Principal. The RCS Network Administrator should make certain the password is changed immediately

Violations

Failure to observe these guidelines may subject users to suspension and or termination of their use of the RCS Network. The RCS Network Administrator will notify the Principal of any inappropriate activities by the users. The Principal will advise law enforcement agencies of illegal activities conducted through the RCS Network and will cooperate fully with local, state, and/or federal officials in any investigation related to illegal activities conducted through the RCS Network.

Disclaimers

The RCS Superintendent, Principal and Network Administrator make no warranties of any kind, either expressed or implied, for the RCS Network's services and resources. The RCS Superintendent, Principal and Network Administrator are not responsible for any damages incurred, including, but not limited to: loss of data resulting from delays or interruption of service, loss of data stored on the RCS

Network resources, or damage to personal property used to access the RCS Network resources; for the accuracy, nature, or quality of information stored on the RCS Network resources or gathered through the RCS Network or the Internet; for unauthorized financial obligations incurred through the RCS Network-provided access. Further, even though the RCS Network may use technical or manual means to limit student access, these limits do not provide a foolproof means for enforcing the provisions of this policy. All provisions of this agreement are subordinate to local, state and federal statutes.