TECHNOLOGY USE, GUIDELINES, AND PROCEDURES

ACCEPTABLE USE POLICY – ACCESS TO ELECTRONIC NETWORKS

Electronic networks, including the Internet, are a part of the District's instructional program and serve to promote educational excellence by facilitating resource sharing, innovation, and communication. The Superintendent shall develop an implementation plan for this policy and appoint system administrator(s). The School District is not responsible for any information that may be lost or damaged, or become unavailable when using the network, or for any information that is retrieved or transmitted via the Internet. Furthermore, the District will not be responsible for any unauthorized charges or fees resulting from access to the Internet.

Curriculum

The use of the District's electronic networks shall: (1) be consistent with the curriculum adopted by the District as well as the varied instructional needs, learning styles, abilities, and developmental levels of the students, and (2) comply with the selection criteria for instructional materials and library resource center materials. Staff members may, consistent with the Superintendent's implementation plan, use the Internet throughout the curriculum. The District's electronic network is part of the curriculum and is not a public forum for general use.

Acceptable Use

All use of the District's electronic networks must be: (1) in support of education and/or research, and be in furtherance of the goals stated herein, or (2) for a legitimate school business purpose. Use is a privilege, not a right. Students and staff members have no expectation of privacy in any material that is stored, transmitted, or received via the District's electronic networks or District computers. General rules for behavior and communications apply when using electronic networks. The District's *Authorization for Electronic Network Access* contains the appropriate uses, ethics, and protocol. Electronic communications and downloaded material, including files deleted from a user's account but not erased, may be monitored or read by school officials.

Internet Safety

Each District computer with Internet access shall have a filtering device that blocks entry to visual depictions that are: (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by federal law and as determined by the Superintendent or designee. The Superintendent or designee shall enforce the use of such filtering devices. An administrator, supervisor, or another authorized person may disable the filtering device for bona fide research or other lawful purposes, provided the person receives prior permission from the Superintendent or system administrator. The Superintendent or designee shall include measures in this policy's implementation plan to address the following:

1. Ensure staff supervision of student access to online electronic networks,
2. Restrict student access to inappropriate matter as well as restricting access to harmful materials,
3. Ensure, to the extent reasonable, student and staff privacy, safety, and security when using electronic communications,
4. Restrict unauthorized access, including "hacking" and other unlawful activities, and
5. Restrict unauthorized disclosure, use, and dissemination of personal identification information, such as names and addresses.

Authorization for Electronic Network Access

Each student and his or her parent(s)/guardian(s) must sign the *Authorization* before being granted unsupervised use. All users of the District's computers to access the Internet shall maintain the confidentiality of student records. Reasonable measures to protect against unreasonable access shall be taken before confidential student information is loaded onto the network. The failure of any student or staff member to follow the terms of the *Authorization for Electronic Network Access*, or this policy, will result in the loss of privileges, disciplinary action, and/or appropriate legal action. *Board Policy 6.235*

All use of electronic network use must be consistent with the school's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. These rules do not attempt to state all required or proscribed behavior by users. However, some specific examples are provided. **The failure of any user to follow these rules will result in the loss of privileges, disciplinary action, and/or appropriate legal action.**

Acceptable Use - Access to the electronic network must be: (a) for education or research, and be consistent with the District's educational objectives, or (b) for legitimate business use.

Privileges - The use of the electronic network is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. The system administrator or Building Principal will make all decisions regarding whether or not a user has violated these procedures and may deny, revoke, or suspend access at any time. His or her decision is final.

Unacceptable Use - The user is responsible for his or her actions and activities involving the network. Some examples of unacceptable uses are:

a. Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any State or federal law;
b. Unauthorized downloading of software, regardless of whether it is copyrighted or de-viruses;
c. Downloading of copyrighted material for other than personal use;
d. Using the network for private financial or commercial gain;
e. Wastefully using resources, such as file space;
f. Hacking or gaining unauthorized access to files, resources, or entities;
g. Invading the privacy of individuals, that includes the unauthorized disclosure, dissemination, and use of information about anyone that is of a personal nature including a photograph;
h. Using another user's account or password;
i. Posting material authored or created by another without his/her consent;
j. Posting anonymous messages;

k. Using the network for commercial or private advertising;
l. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually-oriented, threatening, racially offensive, harassing, or illegal material; and
m. Using the network while access privileges are suspended or revoked.

Network Etiquette - The user is expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

a. Be polite. Do not become abusive in messages to others.
b. Use appropriate language. Do not swear, or use vulgarities or any other inappropriate language.
c. Do not reveal personal information, including the addresses or telephone numbers, of students or colleagues.
d. Recognize that email is not private. People who operate the system have access to all emails. Messages relating to or in support of illegal activities may be reported to the authorities.
e. Do not use the network in any way that would disrupt its use by other users.
f. Consider all communications and information accessible via the network to be private property.

No Warranties - The District makes no warranties of any kind, whether expressed or implied, for the service, it is providing. The District will not be responsible for any damages the user suffers. This includes loss of data resulting from delays, non-deliveries, missed- deliveries, or service interruptions caused by its negligence or the user's errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

Indemnification - The user agrees to indemnify the School District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any violation of these procedures.

Security - Network security is a high priority. If the user can identify a security problem on the Internet, the user must notify the system administrator or Building Principal. Do not demonstrate the problem to other users. Keep your account and password confidential. Do not use another individual's account without written permission from that individual. Attempts to log-on to the Internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the network.

Vandalism - Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any other network. This includes, but is not limited to, the uploading or creation of computer viruses.

Telephone Charges - The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distancee charges, per-minute surcharges, and/or equipment or line costs.

Copyright Web Publishing Rules - Copyright law and District policy prohibit the re-publishing of text or graphics found on the web or on District websites or file servers without explicit written permission.

a. For each re-publication (on a website or file server) of a graphic or a text file that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission was granted. If possible, the notice

   should also include the web address of the original source.
b. Students engaged in producing web pages must provide library media specialists with email or hard copy permissions before the web pages are published. Printed evidence of the status of "public domain" documents must be provided.
c. The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the website displaying the material may not be considered a source of permission.

Use of Email - The District's email system, and its constituent software, hardware, and data files are owned and controlled by the School District. The School District provides email to aid students as an education tool.

a. The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. Unauthorized access by any student to an email account is strictly prohibited.
b. Each person should use the same degree of care in drafting an email message as would be put into a written memorandum or document. Nothing should be transmitted in an email message that would be inappropriate in a letter or memorandum.
c. Electronic messages transmitted via the School District's Internet gateway carry with them an identification of the user's Internet *domain*. This domain is a registered name and identifies the author as being with the School District. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of the School District. Users will be held personally responsible for the content of any and all email messages transmitted to external recipients.
d. Any message received from an unknown sender via the Internet should either be immediately deleted or forwarded to the system administrator. Downloading any file attached to any Internet-based message is prohibited unless the user is certain of that message's authenticity and the nature of the file so transmitted.
e. The use of the School District's email system constitutes consent to these regulations.

Access to Student Networking Passwords & Websites

School officials may conduct an investigation or require a student to cooperate in an investigation if there is specific information about activity on the student's account on a social networking website that violates a school disciplinary rule or policy. In the course of an investigation, the student may be required to share the content that is reported to allow school officials to make a factual determination.

Board Policy 6:235, 7:140

ONE TO ONE TECHNOLOGY

RCS may provide and assign students a computing device for use at school as a means to promote achievement and provide flexible learning opportunities. This policy provides guidelines and information about district expectations for students who are being issued these one-to-one (1:1) computing devices. In addition to this policy, the use of any district-provided technology or network also

requires students to abide by the RCS Acceptable Use Guidelines as stated in the Student Code of Conduct. Additional rules may be added as necessary and will become a part of this policy.

Our expectation and belief are that students will responsibly use district technology and that they understand the appropriate and acceptable use of both the technology and district network resources. We also expect that students will make a good faith effort to keep their district-issued devices safe, secure, and in good working order. Our policies and procedures include the following specific responsibilities and restrictions. The student **WILL**:

1. Adhere to these guidelines each time the device is used.
2. Use responsible, ethical, and polite language in all communications avoiding profanity, obscenity, and offensive or inflammatory speech.
3. Report ALL cyberbullying, including personal attacks or threats toward anyone, made while using either district-owned or personally owned technology, to responsible school personnel.
4. Respect the Internet filtering and security measures included on the laptop. *Note: All student 1:1 computing devices are configured so that Internet content is filtered at school.*
5. Back up important data files regularly. *Note: RCS may need to restore a 1:1 device to factory settings. Students will be notified of this maintenance in advance. All student files not backed up to server storage space or other storage media may be*

   lost during the restoring process. Students should ask for assistance if they do not know how to backup files.
6. Use technology for school-related purposes only during the instructional day while refraining from use related to commercial or political purposes.
7. Follow copyright laws and fair use guidelines and only download or import music, video, or other content that students are authorized or legally permitted to reproduce or use.
8. Make available for inspection by an administrator or teacher any messages or files sent or received to or from any Internet location using district technology. *Note: Files stored and information accessed, downloaded, or transferred on district-owned technology are not private insofar as they may be viewed, monitored, or archived by the district at any time.*

The student **WILL NOT**:

1. Mark, deface, or place stickers on the laptop and/or cases without prior approval from responsible school personnel.
2. Reveal or post identifying personal information, files, or communications to unknown persons through email or other means through the Internet.
3. Attempt to override, bypass, or otherwise change the Internet filtering software, device settings, or network configurations.
4. Attempt access to networks and other technologies beyond their authorized access. This includes attempts to use another person's account and/or password or access secured wireless networks.
5. Share passwords or attempt to discover passwords. *Note: Sharing a password is not permitted and could make you subject to disciplinary action and liable for the actions of others if problems arise with unauthorized use.*
6. Download and/or install any programs, files, or games from the Internet or other sources onto any district-owned technology. *Note: This includes the intentional introduction of computer viruses and other malicious software.*
7. Tamper with computer hardware or software, attempt unauthorized entry into computers, and/or vandalize or destroy the computer or computer files. Intentional or negligent damage to computers or software may result in criminal charges.
8. Attempt to locate, view, share or store any materials that are unacceptable in a school setting. *Note: This includes but is not limited to images, sounds, music, video, language, and other material that are pornographic, obscene, graphically violent, or vulgar. The criteria for acceptability is demonstrated in the types of material made available to students by administrators, teachers, and the school library/innovation center. It is the responsibility of the student to verify the appropriateness of material with responsible school personnel before locating, viewing, sharing, or storing questionable material.*

In addition to the specific requirements and restrictions detailed above, it is expected that students and families will apply common sense to the care and maintenance of district-provided 1:1 technology. To keep the devices secure and damage-free, please follow these additional guidelines:

- Do not loan your 1:1 device or charger and cords.
- Do not leave the 1:1 device unattended at any time.
- Do not eat or drink while using the 1:1 device or have food or drinks nearby.
- Keep your 1:1 device away from precarious locations like table edges, floors, or seats.
- Do not stack objects on top of your 1:1 device, leave it outside, or use near water.

Despite these safeguards, we understand there is always a risk that a district-provided 1:1 device may be damaged, lost, or stolen. If a parent/guardian would like to purchase private insurance, they may. Also, a parent/guardian may choose to purchase a more protective case for the device than the standard case issued by the school district.

RCS is not responsible for any loss resulting from the use of district-issued technology and makes no guarantees that the technology or the district network systems that support student use will be available at all times. By signing this policy you agree to abide by the conditions listed above and assume responsibility for the care and proper use of RCS district-issued device, and you understand that failure to honor the terms of this Policy, access to 1:1 device, the Internet, and technology may result in damage reimbursement fines and disciplinary actions per the Student Code of Conduct