



## **Internet Safety Policy**

# Technology

## **I. Computer/Internet Acceptable Use:**

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 the purpose of 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. Students will be monitored, supervised and educated on safe and appropriate online activities. 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 email. 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.

**Filtering, Monitoring, and Review** – RAS, in order to comply with the local, state, and federal laws and standards, filters internet content on systems to which students, staff, and visitor's may have access. This filtering removes access to websites and internet servers that have been deemed to have an inappropriate content not of an educational value. Report any errors found regarding what sites being, or not being filtered, immediately to an administrator or the Technology Department. RAS retains the right to monitor network, email, computer, and telephone use without warning or notice. Information stored, transmitted, or communicated on RAS equipment is not to be considered private. Information gained through monitoring may be used as evidence in disciplinary or legal action, at the administrator's discretion. RAS retains the right to review current and back-up copies of electronic systems, files, data, communications, and email. Reviews are done without notice, and information gained through review may be used as evidence in disciplinary or legal action should a violation of the Student Acceptable Use of Electronic Networks procedure be discovered.

Filtering can be disabled for legitimate purposes and research. Contact an administrator or RAS Technology Department to have filtering disabled.

**Telephone Charges** - The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance 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. Use of the School District's email system constitutes consent to these regulations.
- f. It must be the student's understanding that RAS provided email is not private or protected. When suspicion of a violation of this procedure pertaining to inappropriate material or usage exists, either through discovery as part of a regular maintenance or by staff, student, or parental complaint, RAS reserves the right to review data and files found on email clients and servers during the course of investigation. Any information gained through this review may be used as evidence in disciplinary or legal action should a violation of this procedure exist.
- g. Unauthorized disclosure, use, and dissemination of personal identification information regarding minors is prohibited.

## **II. Access to Student Social Networking Passwords & Websites:**

School authorities may require a student or his or her parent or guardian to provide a password or other related account information in order to gain access to the student's account or profile on a social networking website if school authorities have reasonable cause to believe that a student's account on a social networking website contains evidence that a student has violated a school disciplinary rule or procedure.

### **Exhibit – Letter to Parents/Guardians Regarding Access to Student Social Networking Passwords and Websites**

*Re: Access to Student Social Networking Passwords and Websites for Violations of School Rules or Procedures*

Dear Parent(s)/Guardian(s):

Under ordinary circumstances, school authorities cannot request or require that a student provide a password or other related account information in order to gain access to the student's account or profile on a social networking website.

School authorities may require a student or his or her parent or guardian to provide a password or other related account information in order to gain access to the student's account or profile on a social networking website if school authorities have reasonable cause to believe that a student's account on a social networking website contains evidence that a student has violated a school disciplinary rule or procedure.

Social networking website means an Internet-based service that allows students to: (1) construct a public or semi-public profile within a bounded system created by the service; (2) create a list of other users with whom they share a connection within the system; and (3) view and navigate their list of connections and those made by others within the system. Social networking website does not include electronic mail.

Please contact the school if you have any questions.

Sincerely,

Principal

Student Service Coordinator

# Authorization for Electronic Network Access Form

Students must have a parent/guardian read and agree to the following before being granted unsupervised access:

All use of the Internet shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. The failure of any user to follow the terms of the **Acceptable Use of Electronic Networks** will result in the loss of privileges, disciplinary action, and/or appropriate legal action. The signatures at the end of this document are legally binding and indicate the parties who signed have read the terms and conditions carefully and understand their significance.

I have read this *Authorization* form. I understand that access is designed for educational purposes and that the District has taken precautions to eliminate controversial material. However, I also recognize it is impossible for the District to restrict access to all controversial and inappropriate materials. I will hold harmless the District, its employees, agents, or Board members, for any harm caused by materials or software obtained via the network. I accept full responsibility for supervision if and when my child's use is not in a school setting. I have discussed the *Acceptable Use of Electronic Networks* with my child. I hereby request that my child be allowed access to the District's electronic network, including the Internet.

---

Parent/Guardian Name (*please print*)

---

Parent/Guardian Signature

Date

Students must also read and agree to the following before being granted unsupervised access:

I understand and will abide by the above *Authorization for Electronic Network Access*. I understand that the District and/or its agents may access and monitor my use of the Internet, including my email and downloaded material, without prior notice to me. I further understand that should I commit any violation, my access privileges may be revoked, and school disciplinary action and/or legal action may be taken. In consideration for using the District's electronic network connection and having access to public networks, I hereby release the School District and its Board members, employees, and agents from any claims and damages arising from my use of, or inability to use the District's electronic network, including the Internet.

---

Student Name (*please print*)

---