Rocklin Unified School District
Employee Authorized
Network, Internet Usage, and E-Mail Privacy
Agreement

Please read this document carefully before signing:

A. Upon employment all individuals permitted to use the Rocklin Unified School District network/on-line services are required to sign the Employee Authorized Network, Internet Usage, and E-Mail Privacy Agreement form and to abide by the terms and conditions of Board Policies 4040 and 6163.4, its corresponding regulations, Children's Internet Protection Act (CIPA), Health Insurance Portability and Accountability Act (HIPAA), state and federal laws, and the policies within.

B. Upon employment each individual permitted to use the Districts computer resources becomes responsible for protecting the resources and data over which he or she has control or access. Computing resources are provided to support the instructional and administrative objectives of the District as well as for academic research. Employees shall be responsible for the appropriate use of technology and shall use the District's resources only for the purpose related to their employment. Employees shall use a standard network code of ethics.

1. Respect the rights of other District network users. Knowingly accessing or sharing data files or e-mail messages without the owner's permission is prohibited.
2. Be polite. Use appropriate language and do not be abusive in your communication to others.
3. Appropriate use should always be legal and ethical, and reflect academic honesty.
4. The District's computer network may not be used to send, download, store, or create e-mail, electronic files, or computer-generated images or sound that contain defamatory, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, or otherwise biased, discriminatory, or illegal material; or violate State, Federal, or District regulations regarding sexual harassment.
5. The use of the District's computers, network equipment, programs, and supplies must be directly related to the employee's work assignment and must not be used for personal/financial gain.
6. The computers, network, and resources are owned and maintained by the District. Personal computers, laptops, PDAs, etc. shall not be connected to the network without the consent of the Management Information Systems Department. There is not a blanket acceptance. Each device will be considered on a case by case basis.

C. User responsibilities include governing/monitoring student use for their protection under the Children's Internet Protection Act (CIPA). In addition to the following policies.

1. Assist in keeping the Districts network free from virus or other malicious attacks by refraining from opening attachments from unknown sources and being alert to all warnings. Do not attempt to bypass, circumvent, or disable network security or virus protection software.
2. Use computer resources responsibly. Do not cause network congestion by sending large files (over 1 megabyte) or sending unwanted or inappropriate e-mail.
3. Use only those computers, applications, and files for which you have authorization.
4. The confidentiality of electronic mail (e-mail) services can not be assured. Therefore, users should exercise extreme caution in using e-mail to communicate confidential or sensitive material. Confidential information should never be sent to outside individuals or agencies not authorized to receive the information. If a confidential e-mail is necessary, the subject line should state "confidential student information." Confidential messages should not be sent or forwarded to others, staff or students, who do not need to know the information. Confidential information should not be sent or forwarded to multiple parties unless there is a clear/legitimate need. Confidential e-mail should not be saved in your personal mailbox, but should be deleted as soon as possible.
5. Except in the line of official school duties and as provided under the Family Educational Rights and Privacy Act (FERPA)*, no student contact information is to be sent via e-mail. This includes the student's name and other information that would allow an individual to locate the student, including but not limited to, parent's name, home address, work address or location, or phone number.

* Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions (34 CFR & 99.31):

a. School official with legitimate educational interest;
b. Other schools to which a student is transferring;
c. Specified officials for audit or evaluation purposes;
d. Appropriate parties in connection with financial aid to a student;
e. Organizations conducting certain studies for or on behalf of the school;
f. Accrediting organizations;
g. To comply with judicial order or lawfully issued subpoena;
h. Appropriate officials in cases of health and safety emergencies; and
i. State and local authorities, within a juvenile justice system, pursuant to specific state law.

D. Anyone with access to student health records will comply with the Health Insurance Portability and Accountability Act (HIPAA) published by the United Stated Department of Health and Human Services, Office of Civil Rights. (http://www.hhs.gov/ocr/hipaa/)

E. Network and e-mail password guidelines. All access to the network is provided by a user name and password. Remember electronic communications are not guaranteed to be private/secure. Therefore, electronic mail and other telecommunications should not be used to share confidential information about students or other employees.

1. Passwords must be kept confidential. ***Do not give out your password. Do not write down your password where others may see it.*** All new users must change their password after their initial login and should change them periodically to ensure confidentiality.
   - Try to create passwords that can be easily remembered. Passwords should be at least 5 characters long. It is a good idea to include numbers and special characters such as '~!@#$%^&*()-_=+{[]}\|`";:,/?. However, do not attempt to substitute numbers or characters that look like the letter they replace (e.g. C@R0L!N@ for CAROLINA); as hackers/password-cracking programs try these combinations first.
   - For maximum security use acronyms of unusual phrases that you invent. An example would be the password "~2myuT$!" for "About 2 more years until Tenure Salary!" Another way to do this is to create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.
   - Do not base your password on any items of personal information (e.g., street address, birthdays, names of family members or animals, and PID, or Social Security number etc.).

2. Internet usage ***is monitored and logged***. Intentional violation of this agreement and the policies as stated within, including searches for hacking, offensive/pornographic or other material, is a violation which will result in privileges being revoked, up to and including, disciplinary and/or legal action being taken.

3. E-Mail is provided by the District and any e-mail sent, received, or stored on a District computer ***is subject to monitoring at any time***. This is to include current and past e-mail messages and all attachments. Violation of this agreement and these policies within will result in privileges being revoked, up to and including, disciplinary and/or legal action being taken.

F. Fair Use and Copyright Issues. The District requires that all proprietary software be purchased and used in accordance with licensing agreements. Copying and/or downloading any commercial software or other material is in violation of this agreement. Do not install software or hardware that does not belong to the District, or properly licensed by the District, (e.g., games, applications, operating systems, “shareware”, Instant Messaging, computer components, and peripherals.) Please see your site computer technician/aide for alternatives, or for District owned hardware/software. File sharing software is strictly forbidden on any District computer.

G. Remote Access. Remote Access is granted to employees for the convenience of completing their job from remote locations. It is the employee's responsibility to ensure that their remote access session remains as secure as their network access at their campus. The remote user agrees to and accepts that access and/or connection to the Districts network may be monitored to record dates, times, duration of access, etc. in order to identify usage patters or suspicious activity. The District will not reimburse employees for their ISP service or any other remote connection charges i.e., hotspot, ISDN, or frame relay charges. Computer and associated programs shall be used **by the employee only** and all rules and regulations within this agreement apply.

Family Educational Rights and Privacy Act (FERPA)

http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Children's Internet Protection Act (CIPA)

http://www.fcc.gov/cgb/consumerfacts/cipa.html

Health Insurance Portability and Accountability Act (HIPAA)

http://www.hhs.gov/ocr/hipaa/

Employee Declaration

Please complete the following information:

I have read and understand the Rocklin Unified School District Employee Authorized Network, Internet Usage, and E-Mail Privacy Agreement. I further understand that any violation of the regulations contained therein is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked and disciplinary action and/or appropriate legal action may be taken.

Print Name: _____

Signature: _____

Site: _____

Date: _____

PLEASE SIGN AND RETURN THIS PAGE TO HUMAN RESOURCES.

RETAIN THE AGREEMENT FOR YOUR REFERENCE.