RIVERSIDE SCHOOL DISTRICT

Parental Signature Form

I have read the Riverside School District's Internet and Technology Acceptable Use Policy. If I do not follow the rules that are in the policy, I understand that my account will be canceled and disciplinary/legal action may be taken.

As a parent/legal guardian, by signing this form, I hereby give permission for my child to keep his/her school account as long as the procedures described by the acceptable use policy are followed.

_____

STUDENT NAME (please print)

_____   _____

STUDENT SIGNATURE   GRADE

_____

PARENT/LEGAL GUARDIAN SIGNATURE

_____

DATE

A PARENT SIGNATURE FORM MUST BE ON FILE AT SCHOOL TO ALLOW STUDENTS ACCESS TO INTERNET AND COMPUTER TECHNOLOGIES.

THANK YOU.

STUDENT ID # _____

STUDENT HOMEROOM # _____

SCHOOL BUILDING _____

ACCEPTABLE USE OF INTERNET

The Riverside School District supports use of the Internet and other computer networks in the instructional program in order to facilitate learning, teaching, and access to information through interpersonal communication, research, and collaboration.

The use of network facilities shall be consistent with the curriculum as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.

The electronic information available to students and staff does not imply endorsement by the Riverside School District of the content, nor does the Riverside School District guarantee the accuracy of information received on the Internet. The Riverside School District shall not be responsible for any information that may be lost, damaged or unavailable when using the network or for any information that is retrieved via the Internet.

 The Riverside School District shall not be responsible for any unauthorized charges or fees resulting from access to the Internet.

The Riverside School District reserves the right to log network use and to monitor fileserver space utilization by users, while respecting the privacy rights of users.

The Riverside School District establishes that use of the Internet is a privilege, not a right; inappropriate, unauthorized or illegal use will result in cancellation of those privileges and appropriate disciplinary action.

The Riverside School District shall make every effort to ensure that its educational resources are used responsibly by students and staff.

The Riverside School District will educate all students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

Students and staff have the responsibility to respect and protect the rights of every other user in the district and on the Internet.

Network accounts shall be used only by the authorized owner of the account for its authorized purpose. All communications and information accessible via the network should be assumed to be private property and shall not be disclosed. Network users shall respect the privacy of other users on the system.

Prohibitions

Students and staff are expected to act in a responsible, ethical and legal manner in accordance with Riverside School District policy, accepted rules of network etiquette, and Federal and State law. Specifically, the following uses are prohibited:

1. Illegal activity.

2. Commercial or for-profit purposes.

3. Non-work or non-school related work

4. Product advertisement or political lobbying

5. Hate mail, discriminatory remarks, and offensive or inflammatory communication.

6. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.

7. Access to obscene or pornographic material.

8. Inappropriate language or profanity.

9. Transmission of material likely to be offensive or objectionable to recipients.

10. Intentional obtaining or modification of files, passwords, and data belonging to other users.

11. Impersonation of another user, use on anonymity, and pseudonyms.

12. Fraudulent copying, communications, or modifications of materials in violation of copyright

    laws.

13. Loading or use of unauthorized games, programs, files or other electronic media.

14. Disruption of the work of other users.

15. Destroying, modifying or abusing network hardware and software.

16. Quoting personal communications in a public forum without the original author's prior consent.

Security

System security is protected through 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, the following 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 teacher'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.

Safety

To the greatest extent possible, users of the network will be protected from harassment and unwanted or unsolicited communication. Any network user who received threatening or unwelcome communications shall immediately bring them to the attention of a teacher or administrator.

Network users shall not reveal personal addresses or telephone numbers to other users on 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 of data belonging to others, copyright violations, or theft of services will be reported to the appropriate legal authorities for possible prosecution.

In addition to the stipulations of this policy, general rules for behavior and communications apply when using the internet. Loss of access and other disciplinary actions shall be consequences for inappropriate use.

Vandalism will result in cancellation of access privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another user, Internet or other networks; this includes but is not limited to uploading or creating computer viruses.

Copyright

The illegal use of copyrighted software by students and staff is prohibited. Any data uploaded from the network shall be subject to fair use guidelines.