



Riverside Unified School District
Acceptable Use Policy for Employee Use of Technology Resources
(Based on Rules and Regulations #4040)

It is the policy of the Riverside Unified School District (RUSD or District) to afford broad access to District computers, communications systems (email, web sites, smart phones, blogging, podcasting and/or other emerging technologies), the Internet and an array of technology resources for District employees for use in fulfilling the District's missions, and for the appropriate District-related activities. The purpose of this Acceptable Use Policy is to outline the acceptable and unacceptable use by employees of District technology resources and personal technology resources that access or use District resources. The principles outlined herein are in place to protect both the employee and the District. This policy applies to all non-student users of the District's technology resources including contractors and affiliated third parties. (Student users of the District's technology resources are governed by a separate Acceptable Use Policy.) It is the sole responsibility of each employee to be informed about his/her responsibilities and the District's expectations for the use of technology resources.

While using District technology resources each employee must act in an appropriate manner consistent with District, ethical and legal principles. This includes any remote access which employees may gain off-site, but which involves the use of District sites, servers, intranet facilities, email accounts, software or equipment. It also includes the use of personal technology resources when such personal resources are utilizing District servers, intranet facilities, email accounts, software or storing or accessing RUSD data.

Access to technology resources carries with it the responsibility for ensuring that the use of these resources is primarily for RUSD purposes and District-related activities, and for maintaining the integrity and security of the District's technology equipment and facilities. The District's communication systems have not been established as a public access service or a public forum. The District has the right to place reasonable restrictions on the material employees access or post through the technology resources. In the interest of making the use of technology resources a natural part of the day-to-day work of all members of the District community, incidental personal use is acceptable. However, the use of District technology resources is prohibited for personal purposes during assigned work time. Use of District technology resources for personal purposes should be incidental, done on the employee's own time, and at the employee's own risk. The District's technology resources shall never be used to solicit commercial sales for personal benefit, religious activities or for political lobbying.

Effective security of technology resources is a team effort that involves the participation and support of every employee. Employees must respect the integrity and security of RUSD's information technology system, and the access privileges, privacy and reasonable preferences of other users. Employees having access to technology resources must take reasonable care to ensure that unauthorized persons are not able to use their access to the system. The use of RUSD technology resources may involve the use of a password, network access code or other identifying or validating code. Such passwords and codes are to be protected as private information provided to the individual user for their sole purpose. Such passwords and codes shall not be disclosed by the employee to others. Employees shall immediately notify Network and Information Systems (NIS) if you have identified a possible security problem. Employees further agree to avoid the inadvertent spread of computer viruses by following the District's virus protection procedures.

The District's technology resources are, by nature, finite. Employees must recognize that certain uses of the District's technology resources may be limited for reasons related to the capacity or security of the District's information technology system, or as required for fulfilling the District's primary instruction and public service missions.

No information technology resources can absolutely guarantee the privacy or confidentiality of electronic data, information and the transmission of such. However, all employees shall take reasonable precautions to protect electronic data, information and the transmission of such containing private and confidential information. The privacy and protection of personally identifiable student and employee data is of paramount importance. Likewise, the safeguarding of physical technology resources assigned to employees is the responsibility of the employee. It is the employee's responsibility to report the loss of private and confidential information, and the loss of technology equipment to the District's Risk Management Department immediately upon the discovery of the loss.

In addition to the general principles set forth in this Acceptable Use Policy, the use of technology resources may be affected by a number of other legal and ethical principles. While it is not possible to list all potentially applicable laws, regulations and local standards, the following are provided:

1. The use of District technology resources may involve the use of a password, network access code or other identifying or validating code. Such passwords and codes are to be protected as private information provided to the individual user for their sole purpose. Such passwords and codes shall not be disclosed by the employee to others.
2. District technology resources shall not be used for any activity, or to transmit any material, that violates United States, California or local laws. This includes, but is not limited to, fraudulent acts, violations of copyright or other intellectual property laws, and any threat or act of intimidation or harassment against another person. RUSD technology resources users may not intentionally create, store, display, print or transmit information which violates the District's Sexual Harassment Policy.

3. District technology resources shall not be used to download, copy, or store any copyrighted software, publications, music, video, or other content without permission from the copyright holder. Any software that is installed on District technology resources shall be properly licensed from the copyright owner thereof, and any modifications must comply with the terms of the applicable license(s). RUSD retains the right to remove software that is not compliant with copyright laws or applicable license(s), or that cause the workstation to become unstable or consume excessive technology resources.
4. The use of District technology resources is not private; employees should not expect that files stored on or transmitted via RUSD's resources will be confidential. All digital transmissions are subject to inspection and/or monitoring by District employees and other officials. Digital storage is RUSD property, and as such, network administrators will review files and communications to maintain system integrity and ensure that employees are using technology responsibly. Data, information and transmissions using District technology resources constitute public records and may be subject to public records retention and release laws.
5. Employees are expected to model tolerance and good manners. District technology resource users agree not to send, access, submit, publish, display or print hate mail, defamatory statements, vulgar, derogatory, obscene, profane, sexually oriented, threatening, offensive or illegal material or language over the Internet or RUSD technology resources, or using RUSD technology resources. District technology resources users shall not access Web sites, newsgroups, or chat areas that contain material that is prohibited under child pornography laws or that promotes illegal acts. The use of District technology resources in a manner intended to injure or humiliate others by disclosure of personal information (whether true or false), personal attacks on others, and statements expressing animus towards any person or group by reason of race, color, religion, national origin, gender, sexual orientation or disability is not acceptable. Cyber bullying is specifically prohibited. It shall be the employee's responsibility to report the inappropriate use, web site, or communication to the employee's supervisor.
6. District technology resources users shall not post anonymous messages or attempt to impersonate another person by forging email, web pages or other electronic media.
7. District technology resources users may not log on to another employee's account, IP address, or other resource access, attempt to access another user's files, or permit anyone else to log on to their own accounts. Users may not try to gain unauthorized access ("hacking") to the files or technology systems of any other person or organization.
8. The primary use of the District's technology resources is for District-related work. While some incidental personal use of the RUSD technology resources is permitted, such incidental use will not be deemed a waiver of District's right to prohibit all such use, either on an individually-applicable or on a generally-applicable basis.

9. District technology resources users shall not use RUSD technology resources to conduct for-profit business activities or to engage in religious or political activities. Employees shall not use District technology resources for advertising, promotion commercial purposes or similar objectives.
10. District technology resources users shall not send unsolicited email messages, including the sending of “junk mail” or other advertising material to individuals who did not specifically request such material (“spamming”). RUSD technology resources users shall not create or forward “chain letters”, “Ponzi” or other “pyramid” schemes of any type.
11. Virtual and physical vandalism shall not be tolerated. Any intentional act by an employee that damages or interferes with performance of District technology hardware, software, operating systems, or communication systems will be considered vandalism and will be subject to discipline and/or appropriate criminal or civil action. RUSD technology resources users shall not introduce malicious programs into the District’s technology resources (e.g. viruses, worms, Trojan horses, email bombs, etc.). District technology resources users shall not intentionally disrupt network traffic or crash the network and connected systems; users shall not degrade or disrupt equipment or system performance.
12. Employees may bring personal technology, including computers, smart phones, network access devices, or other electronic signaling devices to their work place. However, the District is not responsible for the safeguarding of such personal technology.
13. Employees shall not take data, equipment, software or supplies (paper, toner cartridges, disks, etc.) for their own personal use. Such taking will be treated as theft. Employees may take computer equipment home or to off-site destinations for District-related purposes with the prior permission of their supervisor.

RUSD will cooperate fully with local, state and federal officials in any investigation related to any suspected illegal activities conducted through District technology resources.

Employees who violate this Acceptable Use Policy may have their access privileges suspended or revoked. In addition, further disciplinary action may be taken as permitted by applicable law and/or the terms of any applicable collective bargaining agreement.

Notwithstanding the language or descriptions used in this Acceptable Use Policy, Board Policy #4040 and associated administrative rules and regulations govern the use of RUSD technology resources. All employees, contractors and associated third parties shall sign a “User Responsibility Contract” acknowledging receipt of this Acceptable Use Policy and their responsibility to abide by the provisions of Board Policy # 4040, and associated rules and regulations, and this Acceptable Use Policy.

RIVERSIDE UNIFIED SCHOOL DISTRICT

**Acceptable Use of Technology
User Responsibility Contract**

I have **received** the Acceptable Use Policy for Employee Use of Technology Resources. I have **read, understand, and will abide** by the Riverside Unified School District's policies and administrative regulations for the use of technology resources. I further understand that any violation of these policies, administrative regulations for the use of technology resources is unethical and may constitute a criminal offense. Should I commit any violation, my access to privileges may be revoked and disciplinary action and/or other appropriate legal action may be taken.

Employee Name (please print) _____

Employee Signature _____ Date _____

Employee Application for an RUSD E-mail Account

Applicant Name (please print) _____

Social Security Number: _____

Worksite: _____

Work Phone: _____ Home Phone: _____

White Copy--Network Information Systems Yellow Copy--Human Resources Pink Copy--Employee