ROSEVILLE JOINT UNION HIGH SCHOOL DISTRICT
Technology Use Agreement
PREAMBLE

The District acknowledges that the rules and guidelines related to the use of technology in the workplace are evolving and subject to change as practice, legal challenges and legislation emerge to govern this new area. All employees permitted to use the RJUHSD network/on-line services are required to sign this Technology Use Agreement ("Agreement") and to abide by the terms and conditions of Board Policy 4040, its corresponding administrative rules and regulations, and state and federal laws.

These guidelines are intended to protect the legitimate interests of the employer. As an employer, the District has a legitimate interest in:

- Assuring that the network is not used for personal profit or gain or for access to pornography or other uses prohibited by law.
- Assuring that users do not violate the property rights of others.
- Assuring that personal programs are not loaded onto district-owned equipment or networks, unless specifically approved by the District.
- Assuring that work time is not used for personal purposes unless specifically authorized herein.
- Assuring that all electronic "records" are stored on central district staff network file servers (H: and P: Drives, Google Apps for Education Drive) for efficient archival, search and retrieval functions to maintain compliance with public records and litigation hold requirements.
- Assuring that electronic files and data stored off of network file servers (i.e., local hard drives, external or removable storage, etc.) are only used for files that are temporary/transitory in nature.
- Protecting confidential district information, including but not limited to, confidential information pertaining to employees and students.
- Establishing that work created for potential distribution or sale during work time and on district-owned equipment is the property of the District unless the District and employee enter into a specific written agreement designating ownership rights to the employee. The District encourages employees to develop ideas and materials for distribution and looks forward to entering into cooperative ventures with employees to develop ideas and materials for distribution and/or sale.
- Establishing and informing employees that all employee e-mail and Internet usage on district technology is subject to monitoring and review. Online communications are not private, and the District reserves the right to monitor any online communications for improper use.

The District has no desire to prohibit the occasional, de minimis and lawful personal use of the network. The District does not intend to discipline an employee for the occasional use of the network for personal reasons such as the receipt of e-mail from family or friends, or to conduct occasional personal business. Employees may use the district network to communicate with others as long as that use does not intrude on the work environment; does not jeopardize the security of the District's employees, network, equipment or any sensitive student or organizational data; and does not violate any applicable laws or district policies. The following guidelines are intended to assist employees in using the electronic information resources. The District will be guided by principles of reasonableness, the due process rights of employees and the emergence of legal standards related to the employee use of district technology.

GUIDELINES

Permitted Use (Acceptable Use)

Employees may use the District's electronic information resources to conduct the business of the District. Examples of such use include:

- The exchange of business-related information.
- The research of topics reasonably related to the established curriculum or to the operations of the District.
- The sharing of instructional strategies and practices.
- The lawful correspondence among employees, as long as that correspondence does not interfere with the employee's assigned work hours, duties and performance expectation.

Additionally, the District does not prohibit the occasional, de minimis and reasonable personal use of email and the Internet as long as that use does not interfere with the employee's assigned work hours, duties and performance expectations. Such use is subject to review and monitoring by the employee's supervisor and the District, and employees should have no expectation of privacy for any personal use or communication. Personal use of the District's technology resources beyond occasional de minimis use, whether during business hours or after hours, is not allowed.

Users should exercise extreme caution in using e-mail to communicate confidential or sensitive district information including, but not limited to, confidential employee information and confidential student and parent information ("Confidential Information"). Confidential Information should never be sent to outside individuals or agencies not authorized to receive it. If a confidential e-mail is necessary, the subject line should state "Confidential 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-mails should not be saved in personal mailboxes and should be retained in accordance with the District's records retention Board Policy/Administrative Reg. 3580.

Confidential Information related to students ("Confidential Student Information") is protected by both state and federal laws. (See Education Code §49062 et seq. and 34 C.F.R. §99.31.) Employee use of technology for transmission of Confidential Student Information to individuals authorized to receive such information shall comply with Board Policy/Administrative Reg. 5125. Prior to transmitting Confidential Student Information within the scope of employment, employees are responsible for familiarizing themselves with Board Policy/Administrative Reg. 5125. Any questions concerning the permissible transmission of Confidential Student Information shall be addressed with the Assistant Superintendent, Curriculum and Instruction.

Social Media: The District recognizes there are legitimate professional reasons for using social media at work or using district technology resources to access social media. To enable employees to take advantage of the professional value of these sites and to promote an open, trusting, collaborative workplace, RJUHSD allows employees to use social media within the guidelines specified in Board Policy/Administrative Reg. 1114.

Internet Applications: Websites as well as Internet applications, often referred to as "Apps", collect different amounts of information. Apps contain terms of use which are contractual commitments between the user of the Apps and the Apps providers. When a user agrees to the terms of service of websites or Apps, he/she is entering into an agreement with that company as an individual and not as a representative of the District since only the District Board may approve district contractual agreements. To protect staff and student information, all Apps used by employees involving Confidential Information must be approved by the Technology Services Department and authorized by the District pursuant to a contract that is approved by the District Board.

Prohibited Acts/Conduct

- Unsecured transmitting of any confidential or sensitive student and/or organizational data outside of the District. Such transmission is prohibited and can be illegal. This includes email, chat, texting, instant messaging and other modes of communication. Employees who transmit any student or staff data electronically outside the District are to contact the Technology Services Department to ensure proper precautions are being followed.
- Accessing, viewing, downloading or transmitting any pornographic or obscene material.
- Transmitting any illegal, pornographic or inappropriate content, whether internal or outside the District. Such transmission is prohibited and can be illegal, even if the intent is to notify or inform the proper staff/authorities. Employees are to contact their immediate supervisor and work with the Technology Services and/or Personnel Services Departments as needed.
- Sharing account username and password. All technology use and correspondence must be conducted under the identity and user account established for the employee by the District.
- Impersonating another person or sending a communication under a false or unauthorized name.
- Violating or attempting to violate another person's privacy including, but not limited to, providing, accessing or using another user's account, identification number, password, electronic files, data or email. Transmitting personal or financial information about others is not permitted. Employees should use great caution when providing personal information about themselves.
- Using computer resources that violate copyright, trademark or license agreements.
- Circumventing or attempting to circumvent local or network security measures.
- Damaging or attempting to damage equipment, software or data belonging to the District or others.
- Tampering or attempting to tamper with any protections or restrictions placed on computer applications and files, including attempting to gain access to any restricted data or files.
- Altering or attempting to alter system software or hardware configurations on either network systems or local computing devices.
- Installing unauthorized software programs or programs not properly licensed on district-owned networks or computing devices. Downloading of any programs or software onto district equipment must have prior approval from the Technology Services Department. All downloaded data must be scanned for viruses.
- Sending or storing messages and/or materials that threaten, harass, defraud or defame others.
- Using district resources for commercial purposes or for personal financial gain. Work created for potential distribution or sale during work time is the property of the District unless the District and employee enter into a specific written agreement designating ownership rights to the employee.
- Any use of technology that violates state, federal or local law.

The above list is not to be considered exhaustive. Employees are required to obtain prior approval from their supervisor for any use of the District's electronic information resources not expressly authorized above. Additionally, employees are encouraged to contact their supervisor if they are unsure if a specific use may be categorized as a prohibited use. Employee conditional use of district technological resources including computers, e-mail, network and access to the Internet shall be permitted within this policy and applicable board policies and administrative regulations.

Consequences for Misuse

Subject to the due process provisions established in law and in the applicable collective bargaining agreements, employees may be disciplined for abuse or misuse of the District's electronic information resources. Such discipline may include provisions up to and including a suspension without pay and/or a recommendation for dismissal.

Acknowledgement of Receipt of Guidelines

My signature below indicates that I have read, understand and agree to abide by all guidelines enumerated above.

Employee Name *(please print)* _____ Site _____

Employee Signature _____ Date _____

Federal Law Resources:
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