SAN LORENZO
UNIFIED SCHOOL DISTRICT
BOARD POLICY

Human Resources BP 4040(a)

EMPLOYEE RESPONSIBLE TECHNOLOGY USE

The Governing Board recognizes that technological resources can enhance employee performance, engage learners, and increase student achievement by offering effective tools to assist in providing a quality instructional program, facilitating communications with parents/guardians, students, and the community, supporting District and school operations, and improving access to and exchange of information. The Board expects all employees to learn to use the available technological resources that will assist them in the performance of their job responsibilities. As needed, employees shall receive professional development in the appropriate use of these resources.

Employees shall be responsible for the appropriate use of technology and shall use the District's technological resources primarily for purposes related to their employment.

Employees shall have no expectation of privacy with regard to computer equipment, electronic data and files, and electronic communications, including email, voice mail, mobile technologies, blogging and social media use. Unless authorized by a direct supervisor, Superintendent or designee, technological resources shall not be used to transmit confidential information about students, employees, or District operations.

The Superintendent or designee shall ensure that each District computer with internet access has a technology protection measure that prevents access to child pornography and visual depictions that are obscene or otherwise harmful to children, and shall enforce the use of such measure. The Superintendent or designee may disable the technology protection measure during use by an adult to enable access for bona fide research or other lawful purpose. (20 USC 6777; 47 USC 254)

The Governing Board acknowledges that inappropriate activity on computer networks and the internet poses a potential threat to the individual and can result in accessing material that is not suited for the public educational system. The intent of San Lorenzo Unified School District is to provide internet access to enhance professional/educational usage and increased communication. The District System may not be used for commercial or “for profit” services.

The Superintendent or designee reserves the right to monitor employee usage of technological resources, including the accessing by any person of email and stored files. Monitoring may occur at any time without advance notice or consent.

The Superintendent or designee shall establish administrative regulations and a Responsible Technology Use (“RTU”) Agreement which outlines employee obligations and responsibilities related to the use of District technology. The Superintendent or designee also may establish guidelines and limits on the use of technological resources. Inappropriate use may result in a cancellation of the employee's user privileges, disciplinary action, and/or legal action in accordance with law, Board policy, and administrative regulation.

EMPLOYEE RESPONSIBLE TECHNOLOGY USE

All employees must adhere to these guidelines which will create an educational environment which encourages user access and promotes a safe and secure atmosphere for learning.

The Superintendent or designee shall provide copies of related policies, regulations, and guidelines to all employees who use the District's technological resources. Employees shall be required to agree in writing that they have read and understood the District's Responsible Technology Use policy.

Use of Personal Cellular Phone or Mobile Communications Device

An employee shall not use a cellular phone or other mobile communications device for personal business while on duty, except in emergency situations and/or during scheduled work breaks.

With prior authorization, employees may use personal cell phones or mobile communications devices for educational purposes in the classroom and have access to a segmented network for internet access provided by the district. The personal phone or device must be approved and configured by the District to align with the District system.

Any employee that uses a cell phone or mobile communications device in violation of law, Board policy, or administrative regulation shall be subject to discipline and may be referred to law enforcement officials as appropriate.

(cf.110 – Violations of Board Policies/Sanctions)

Legal Reference:

Education Code
51870-51874 Education technology
52270-52272 Education technology and professional development grants
52295.10-52295.55 Implementation of Enhancing Education Through Technology grant program
Government Code
3543.1 Rights of employee organizations
Penal Code
502 Computer crimes, remedies
632 Eavesdropping on or recording confidential communications
Vehicle Code
23123 Wireless telephones in vehicles
23123.5 Mobile communication devices; text messaging while driving
23125 Wireless telephones in school buses
United States Code Title 20
6751-6777 Enhancing Education Through Technology Act, Title II, Part D, especially:-6777 Internet safety
United States Code, Title 47
254 Universal service discounts (E-rate)
Code of Federal Regulations, Title 47
54.520 Internet safety policy and technology protection measures, E-rate discounts

Management Resources:

Websites
CSBA: http://www.csba.org
American Library Association: http://www.ala.org
California Department of Education: http://www.cde.ca.gov
Federal Communications Commission: http://www.fcc.gov
U.S. Department of Education: http://www.ed.gov

SAN LORENZO
UNIFIED SCHOOL DISTRICT
ADMINISTRATIVE REGULATION

Human Resources AR 4040(a)

EMPLOYEE RESPONSIBLE TECHNOLOGY USE

I. DEFINITIONS

A. "District System" means all related District owned electronic technology including but not limited to computers, related hardware and software services, networks (intranet) and internet access including e-mail.

B. "Internet access" means any and all access to the internet provided through the District Systems including, but not limited to, remote access to the District's computer servers.

C. "Employee" means any person who is being paid for their services out of district funds.

II. GENERAL PROVISIONS

A. The San Lorenzo Unified School District ("District") provides employees with access to the District System with the primary intent and purpose of fostering the educational mission of the District reflected in Board Policy, the District wide Goals/Objectives and the District's Blueprint for Success. The System will be used to increase and improve communication within the District; support the District's mission, goals and objectives; enhance productivity; and assist District employees in upgrading their skills through greater exchange of information with their peers. The District System will also assist the District in sharing information with the local community, including parents, social service agencies, government agencies, and businesses. The use of the District System for communication on issues pertaining to professional organizations and employee associa-tion business is allowed, but will be subject to reasonable regulation by the District.

B. This regulation will govern use of the District System by District employees as indicated in Board Policy 4040. Before any employee uses the District System, the employee must review and agree to abide by the terms and conditions of this regulation by signing the District's Responsible Use ("RTU") Agreement (Exhibit A). If an employee fails to sign the RTU and uses the District System, that employee is nonetheless bound by the terms and conditions of this regulation.

EMPLOYEE RESPONSIBLE TECHNOLOGY USE (continued)

III. RESPONSIBLE USE & USE RESTRICTIONS

A. Access to the District System, including networks and the internet, through school resources, provides a professional communication "tool" and is a privilege granted by the District. Network user accounts will be used only by the authorized owners of the accounts for authorized purposes. Inappropriate, unauthorized and illegal use will result in the revocation of the privilege and appropriate disciplinary action. Employees are responsible for damages to equipment, Systems, and software resulting from unauthorized acts to the extent authorized by law.

B. Employees shall support the District's educational mission by using the District System for classroom activities, professional or career development, and educational training, and to support the District's curriculum, policy and mission statement as well as the business function of the District.

C. When using the internet for class activities, teachers will select material that is appropriate in light of the age of the students and that is relevant to the course objectives. Teachers will preview the materials and sites they require or recommend students access to determine the appropriateness of the material contained on or accessed through the site. However, in the interest of providing students with opportunities to enhance their research skills, it may be appropriate to allow students access to a wide variety of unpreviewed web sites which are relevant to and specifically address research or class related assignments. Employees shall provide prudent and reasonable supervision under the circumstances for students who are using the District System to access the internet. Teacher aides and student aides may be asked to assist in such supervision. The purpose of such supervision shall be instructional as well as to prevent students from misuse of the District System.

D. The District has software and systems in place that monitor and record internet usage on the District System. District security systems are capable of recording (for each and every user) each World Wide Web site visit, each chat, newsgroup or e-mail message, and each file transfer into and out of District internal networks, and the District reserves the right to monitor such usage at any time. No employee has any right to expect privacy as to his or her internet usage while using the District System. District managers will review internet activity and analyze usage patterns, to assure that District internet resources are devoted to maintaining the highest levels of productivity and are being used strictly in accordance with the terms and conditions of this regulation.

E. District departments and school sites that wish to publish on the San Lorenzo Unified School District website must submit the *School Site/Department Web Page Supervisor Agreement* to be kept on file in the Educational Technology/Instructional Materials Center or the School Site. Materials that have been approved by the Ed Tech Department or the *School Site/Department with a current Web Page Supervisor and Social Media Supervisor Agreement* will be posted on the District Website. If material on the district or school site websites is deemed inappropriate by the Superintendent or designee, it can be taken down by the District Webmaster.

F. Use Restrictions

1. Employees may not use the District System to download or distribute pirated software or data.

2. Employees shall use the District System safely, responsibly, and primarily for work related purposes.

3. Employees may not use the District System to propagate any virus, worm, Trojan Horse, trap-door program code, or any other malicious, disruptive, or disabling program.

4. Employees may not use the District System to disable or overload any computer System or network, or to circumvent, disable or destroy any System intended to protect the privacy or security of another user of the District System.

5. Employees shall not access, post, submit, print, send, publish, or display harmful or inappropriate matter that is threatening, obscene, disruptive, or sexually explicit, or that could be construed as harassment or disparagement of others based on their race, ethnicity, national origin, sex, gender, sexual orientation, age, disability, religion, or political beliefs, or any other basis prohibited by law.

6. Employees shall not attempt to gain unauthorized access to the District System or to any other computer system through the District System, or exceed their authorized access, including attempting to log in through another person's account or access another person's files without authorization.

7. Employees may access the internet through the District for incidental non-business research, browsing or purchasing for personal use during meal times or other breaks, or outside of work hours, provided that all other usage policies are adhered to and District work or business is not interrupted, displaced or in any material way interfered with.

8. Employees may not use the District System to download images, videos or games unless there is an express District business-related or educational use for the material.

9. Employees may use the District System to download software only for direct District business use, and must arrange to have such software properly licensed and registered. Downloaded software must be used only under the terms of its license and must be approved by the Superintendent or designee. Employees with internet access may not upload any software licensed to the District or data owned or licensed by the District without the express authorization of the manager responsible for the software or data.

10. Employees shall not provide access to the District System or internet access to unauthorized individuals.

EMPLOYEE RESPONSIBLE TECHNOLOGY USE (continued)

11. Employees shall not use the District System to promote unethical practices or any activity prohibited by law, Board policy, or administrative regulations.

12. Copyrighted material shall be posted online only in accordance with applicable copyright laws.

13. Employees shall not use obscene or threatening language in communications transmitted through the District System. Restrictions against obscene or threatening language apply to public messages, private messages, and material posted on internet pages.

14. Employees shall not use the District System for the purpose of harassing another person. If an employee is requested by another person to stop sending the other person messages, documents or other information over the District System because the person is feeling harassed, the employee must immediately stop sending the other person messages. Any disputes over the "harassing" nature of such communications shall be resolved by the Superintendent or designee.

15. Employees must not knowingly or recklessly post false or defamatory information about another person or organization. Such limitations on employee communication shall be resolved by the Superintendent or designee.

G. Illegal Acts

1. The District's System must not be used in violation of any local, state, federal, or international laws or regulations Employees may not use the District System to engage in any illegal act, including but not limited to arranging for the purchase or sale of illegal drugs, engaging in criminal gang activity, making a terroristic threat, misusing, vandalizing or misappropriating District property, assets or resources, misappropriating intellectual property, or in any other way threatening the health, safety or welfare of another person or property. Use of any District resources for illegal activity is grounds for discipline including immediate dismissal, and the District will cooperate with any legitimate law enforcement effort to prosecute any such illegal activity.

2. Federal copyright laws on apply to the use of material accessed through the District System. Violations of copyright law include, but are not limited to, the unauthorized copying, distribution, use and/or installation of protected works, materials, or software.

3. Laws and professional standards of conduct pertaining to plagiarism must be followed. Plagiarism is defined as the taking of ideas or writings of another person and presenting it as the original ideas of writings of the taker.

4. Altering any communication originally received from another person or computer with the intent to deceive is prohibited.

EMPLOYEE RESPONSIBLE TECHNOLOGY USE (continued)

H. Sexual Harassment Policy Violations

1. Sexually explicit, obscene or profane material may not be accessed, archived, stored, distributed, edited or recorded using the District System. The display of any kind of sexually explicit, obscene or profane image or document on any District System is a violation of District policy on sexual harassment. (Example: derogatory or sexual photographs, cartoons, drawings, sexual innuendos, slurs.)

2. The District uses independently supplied software and data to identify inappropriate or sexually explicit internet sites. The District may block access from within the District System to all such known sites. Any employee who connects accidentally to a site that contains sexually explicit or offensive material must disconnect from that site immediately, regardless of whether that site has been previously deemed acceptable by any screening or rating program, and should immediately notify his or her supervisor and/or the Superintendent or designee.

I. Commercial Purposes

Employees may not use the District System for private commercial purposes or financial gain, defined as offering or providing goods or services, or advertising, in the course of operating any private commercial enterprise in which they have a financial or proprietary interest, or in which members of their families have financial or proprietary interests. District acquisition policies will be followed for District purchase of goods or services through the District System.

J. Political Lobbying/Fundraising

Employees may not use the District System to urge support or defeat of a ballot measure or candidate. Political fundraising or unauthorized use of the District name in association with political activities on the District System is prohibited. Employees may not solicit others, including coworkers, to make financial contributions or other contributions, such as services or goods, to causes, charities or organizations, whether for-profit or non-profit, via the District System, unless expressly authorized to do so by the–Associate Superintendent of Business or designee.

K. Personal Information

1. Each employee using the District System shall identify himself or herself honestly, accurately and completely–in his/her online communications. Employees are prohibited from misrepresenting their identity when it is associated with the District.

2. Employees shall not post personal contact information about other people on or through the District System and shall hold the District harmless if they choose to reveal personal contact information about themselves.

3. Unless there is a legitimate educational purpose for doing so, no information of any kind regarding the physical location of any District student shall be disseminated on the District System without express authorization from an immediate supervisor or authorized manager.

4. Employees who wish to publish their work or image on the District web page will first fill out the *Employee Work Release Form for Internet Web Project/Image Publishing*. This form will be forwarded and kept on file in Human Resources, along with the signed RTU (Exhibit A).

L. Confidential Information

1. Employees are prohibited from revealing the following on the District System: confidential District information, confidential employee and student data, and any other material made confidential by law or existing District policies and regulations. Employees releasing such confidential information via the District System will be subject to the penalties provided in law and existing District policies and regulations.

2. Employee IDs and passwords help maintain individual accountability for internet resource usage. Employees must keep passwords confidential and must take all reasonable precautions to prevent others from being able to use their account, except in authorized situations for District-related purposes. The sharing of user IDs or passwords obtained for access to the District System is prohibited except as expressly authorized by District supervisors.

M. District Authorization

Only those employees or officials who are authorized to speak to the media, to analysts or at public gatherings on behalf of the District may speak and/or write on behalf of the District to any newsgroup, chat room, bulletin board, user comments or by using e-mail. Other employees may participate in newsgroups or chats in the course of business when relevant to their duties, but they may only do so as individuals speaking for themselves.

N. Social Media Use

1. Social Media can be used as a powerful educational resource and communication tool if used correctly and appropriately. Social media includes, but is not limited to, Flickr, Facebook, Twitter, Linked In, YouTube, WordPress, TeacherTube, Instagram, etc.

2. Curricular Use

   a) An employee must notify his/her supervisor if he/she plans to create an account using Social Media specifically for curricular purposes. In such cases, the District may monitor the Social Media account or use at any time without advance notice or consent.

   b) An employee is responsible for monitoring student use of Social Media that has been incorporated into curriculum in order to promote and evaluate the instructional or educational purpose and ensure compliance with the District's Social Media Policy for Students.

   c) If an employee creates or uses an online account for educational purposes, the employee shall be required to provide their login or password for the accounts generated for educational purposes if the District reasonably believes that the online information is relevant to an investigation of alleged employee misconduct or violation of applicable laws and regulations.

3. Communications on Social Media

   a) Employees should not communicate with current District students through Social Media sites unless it is for an instructional or educational purpose. Employees should be mindful about maintaining appropriate professional boundaries with District students and other minor children at all times while utilizing Social Media.

   b) If, through Social Media usage described in this Regulation, an employee becomes aware of known or suspected child abuse or neglect, a threat of harm to a minor or others, or evidence of a crime related to the District, the employee should immediately notify the appropriate authorities and Administrator, Superintendent or designee and comply with his/her obligations under the Child Abuse and Neglect Reporting Act.

   c) Communications through Social Media are not private and employee must not share confidential information concerning District employees, students and families. Social Media may not be used to publish student information including, but not limited to, names, assignments, grades attendance data, photographs, videos, or to her likenesses, without the permission of the students' parents or guardian. (See Student Responsible Use Policy)

   d) Employees are responsible for their Social Media use and may be subject to civil liability if such use is found defamatory, harassing, discriminatory, threatening, or in violation of any applicable law, policy, or regulation. Employees may also be liable if they use confidential or copyrighted information belonging to others. All such postings are prohibited under this policy. The District shall not reimburse employees for any errors, omissions, loss, or damage claimed or incurred due to Social Media use.

e) Employee use of Social Media within the course and scope of their employment is a privilege, and not a right. As such, employee use of Social Media shall be contingent upon compliance with the District's Responsible Use Policy and any applicable state and federal laws, and other District Policies and Administrative Regulations.

4. District Logos and Trademarks: The logos and trademarks of the District and its schools may be used only on official District or school internet sites or publications and in emails delivered through the District email system by current staff members. Any other use of the District or school logo or trademark is prohibited unless prior written permission is obtained from the Superintendent or designee.

5. Notice of Discipline/Violation

a) Failure to comply with these policies may result in discipline, up to and including dismissal, in accordance with collective bargaining agreements, Board Policies, Personnel Commission Rules and Regulations and state law.

b) If an employee witnesses a policy violation, the employee should report the incident immediately to his/her supervisor.

O. Bring Your Own Device

1. With the approval of an immediate supervisor, an employee may use the District System and Internet Access with his/her own mobile device or computing device. This use is a privilege, not a right, and an employee's inappropriate use will result in the revoking of the privilege at the District's discretion.

2. If an employee uses the District System or Internet Access with his/her own device, the District will not be responsible for any damages that may be caused to the employee as a result. This includes loss of equipment, loss of data resulting from delays, non-deliveries, or service interruptions caused by the District System or its operator. An employee's use of information obtained through the District System or Internet Access is at his/her own risk.

3. If an employee uses the District System or Internet Access with his/her own device, the District shall not be obligated to provide any technology support beyond the information needed to connect to the Internet.

P. Cloud Computing

Cloud computing is a general term for anything that involves delivering hosted services over the Internet by a third party, not the District and not the staff member. Cloud computing entrusts remote services with a user's data, software and computation.

All cloud services reserve the right to monitor communications transmitted through their services. As a result, all information placed on the cloud system provided by the district should be considered open and available to the public in perpetuity.

All employees who use the cloud service provided by the district should expect to be subjected to advertisements as a related cost of the service.

In order to protect our students' and employees' confidential records, cloud services must only be used to store student and teacher files for educational and learning purposes.

1. All employees who use the cloud service must never upload confidential student records information, including but not limited to contact information, IEP language, transcripts, discipline records, 504 documentation, accommodations or modification language, or grades.
2. All employees who use the cloud service must never upload confidential personnel information, including but not limited to contact information, evaluations, discipline records, employment history, coaching memos, or letters of reprimand.

Q. Reporting Misuse

Employees must immediately notify their supervisor or the Superintendent or designee once they identify a possible security problem or breach of District Policy.

IV. SECURITY

A. The District has installed an internet firewall to assure the safety and security of the District's networks. Any employee who attempts to disable, defeat or circumvent any District System security may be subject to discipline, including immediate dismissal, and criminal prosecution.

B. For the protection of the District's work environment, only those internet services and functions with documented business purposes for the District will be enabled at the internet firewall.

C. Any file that is downloaded must be scanned by district antivirus software for viruses and worms before it is run or accessed. Employees must avoid the inadvertent spread of computer viruses and worms by following all applicable District protection procedures. The Information Technology Department will provide guidance and assistance as needed.

EMPLOYEE RESPONSIBLE TECHNOLOGY USE (continued)

V. RESOURCE LIMITS

A. Due to the limited capacity of the District System, employees should abide by the following resource-conservation guidelines:

1. Employees shall not post chain letters or engage in "spamming," which is defined as sending a non-District business related message or messages to a large number of people, which disrupts employees' work and overloads the District System.

2. Employees must check their e-mail frequently, delete unwanted or unnecessary messages promptly, and stay within any established e-mail quota.

3. Employees should not stream videos or music while connected to the District System.

B. Employees may not subscribe to online services or solicit information that incurs a cost to be borne by the District unless expressly authorized to do so by their supervisors or job descriptions.

C. All electronic files and file space maintained by or assigned to any employee, volunteer or other individual who has retired, resigned or otherwise separated from the District may be remove or deleted by the District immediately upon such separation from the District to the extent permitted by law.

VI. LIMITATION OF LIABILITY

A. The District makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the District System will be error-free or without defect. The District shall not be responsible for any information that may be lost, damaged or unavailable when using the District System or for any information that is retrieved by accessing the internet. The District does not endorse the content of information available to employees over the internet, nor does the District guarantee the accuracy or quality of information obtained through the internet or stored on the District System.

B. The District shall not be responsible for any unauthorized charges or fees incurred by employees from access to the internet. The District shall not be responsible for financial obligations arising through the unauthorized use of the District System.

EXHIBIT A

EMPLOYEE RESPONSIBLE TECHNOLOGY USE

I acknowledge that I have received a written copy of the Administrative Regulation 4040, also known as the Responsible Technology Use Policy ("RTU") for the San Lorenzo Unified School District

I understand the terms of this RTU policy, which are incorporated herein by reference as though fully set forth in this Agreement, and I hereby agree to abide by them.

I understand that by using the District System I have no expectation of privacy and the District's security software may monitor my use of the internet and other portions of the District System and examine all System activities that I participate in, including but not limited to accessing and storing the e-mail messages I send and receive, the internet addresses of any sites that I visit, and any network activity in which I transmit or receive any kind of file.

I hereby waive any privacy expectation I may have with regard to my use of the District System and as to any communications I transmit or receive through the District System.

I understand that any violation of this RTU policy could lead to my discipline or dismissal from District employment as well as civil and/or criminal prosecution.

_____

Date

_____

Signature

_____

Name (*Please Print*)

EXHIBIT B

San Lorenzo Unified School District
School Site/Department Web Page/Social Media Supervisor Agreement

Web publishing offers a communications resource that can build community awareness and support. Web-based publishing also increases communications and provides access to the site webpage, but also any social media accounts opened in the name of the district/school site.

Each site and department creating webpages and/or social media accounts must designate an **employee webpage supervisor** and/or **social media supervisor** whose role is to approve the content of the school site or department web pages and social media sites and certify that all District policies regarding use of electronic resources and web publishing are followed (AR 4040; BP 6163.4; AR 6163.4).

Each school site's website is maintained by a district webpage supervisor who can change the content to reflect district goals at any time.

SCHOOL SITE or DEPARTMENT: _____

PRINCIPAL: _____

NAME OF DESIGNATED WEB PAGE SUPERVISOR: _____

NAME OF DESIGNATED SOCIAL MEDIA SUPERVISOR: _____

POSITION: _____

Social Media webpages we are using at our site: _____

I, _____, (please print) am responsible for the use of the site/department web publishing. I will certify that District policies regarding web publication and responsible use are followed.

I, _____, (please print) am responsible for the use of the site/department social media publishing. I will certify that District policies regarding web publication and responsible use are followed.

Site or Department WEB SUPERVISOR SIGNATURE	PRINCIPAL SIGNATURE
DATE: _____	DATE: _____
SOCIAL MEDIA SUPERVISOR SIGNATURE	PRINCIPAL SIGNATURE
DATE: _____	DATE: _____

Please route a copy of this agreement to the Educational Technology Department at the District Office. A copy must be on file before a password is assigned and training provided. NOTE: Administrative Regulations and Board Policies related to responsible use of electronic resources are available as a packet from the Educational Technology/Instructional Materials Center or may be found on the District web site.

San Lorenzo Unified School District

Employee Work Release Form: Internet Web Project Publishing

The San Lorenzo Unified School District, specifically _____ (department/school), may be creating web pages to display and disseminate District related information and communications over the internet through the publishing of web pages.

Employees will **always** be asked for permission to display any original written information or personal image before it is published on a web page or presented in an electronic version that can be accessed through the Internet. The work will be accessible to anyone who is connected to the internet/intranet with a web browser. Personal information, such as name **will not** be published without permission to do so; no personal addresses or phone numbers will be published on District web pages.

Please indicate whether or not you would like your **work or image** to be displayed on the District sponsored web pages by filling in the sections below.

Permission to display employee work on District web pages

I, the undersigned, hereby **authorize** the San Lorenzo Unified School District to display my work on a District web page. I understand that my name will not be used without permission, and personal information will not be included. I understand that this work is accessible to anyone who is connected to the internet/Intranet and the ownership of intellectual property cannot be guaranteed. I agree to hold harmless San Lorenzo Unified School District, its Board of Trustees, officers, agents, and employees from and against all costs (including attorney's fees and costs), losses, claims demands, suits, and actions arising from any misuse of the work (copy attached).

NAME/Employee:_____ **Employee Signature:** _____

District Position: _____ **Date:** _____

Permission to Use Employee Image

I understand that my image may be published on the World Wide Web, a part of the internet, as a part of a District web page. An image could take the form of a photograph, video, or multimedia project. **No name, home address or telephone number** will appear with such image. I give permission for publishing my image, and I agree to hold harmless San Lorenzo Unified School District, its Board of Trustees, officers, agents, and employees from and against all costs (including attorney's fees and costs), losses, claims, demands, suits, and actions arising from any misuse of the image (copy attached).

Employee Signature: _____ **Date:** _____

Permission to Use Employee Name

I give permission for my image to appear on the District web site and also give permission to use my name and/or position with it. I agree to hold harmless San Lorenzo Unified School District, its Board of Trustees, officers, agents, and employees from and against all costs (including attorney's fees and costs), losses, claims, demands, suits, and actions arising from any misuse of the image.

Employee Name: _____ **Position:** _____ **Date:** _____

Name to be used: _____ **Signature:** _____