Lucia Mar Unified School District

ACCEPTABLE USE POLICY AND COMPUTER USE AGREEMENT

TERMS AND CONDITIONS FOR USE OF COMPUTER RESOURCES

The Board of Education and the Superintendent of Lucia Mar Unified School District recognize that technology plays a critical role in educating students, enhancing employee performance and facilitating communication between the District, teachers, parents and students. Responsible and appropriate use of technology is essential to productive work and educational environments.

The District's Acceptable Use Policy ("AUP") is to prevent unauthorized access and other unlawful activities by users online, prevent unauthorized disclosure of or access to sensitive information, and to comply with the Children's Internet Protection Act ("CIPA"). The AUP applies regardless of the physical location of a user, the AUP applies when District equipment is used off of District property, and the AUP applies when district resources are accessed using personal or other non-District devices whether on or off District property.

This Acceptable Use Policy and Computer Use Agreement ("Agreement") sets forth the rules and regulations that all District employees and students must follow. Each user of the District's computer resources agrees to the conditions established herein. It is the responsibility of every computer user to know these rules and regulations and to conduct activities accordingly.

SECTION 1.
PREAMBLE

The Lucia Mar Unified School District's ("District") computer resources are provided subject to the rules and regulations set forth in this Agreement.

As a condition of using District computer resources, all users must sign the written "Computer Use Agreement" and by doing so acknowledge that he/she has read and understands the terms of this Agreement and agrees to abide by all terms and obligations herein. Use of District computer resources in violation of this Agreement is prohibited. A user who violates the terms of the Agreement will be subject to revocation or suspension of the privilege of using the District's computer resources and may be subject to appropriate discipline.

SECTION 2.
DEFINITION OF TERMS

Computer resources: The sum total of all computers, the district's computer network including servers and wireless computer networking technology (wi-fi), the Internet, cloud-based applications, email, USB drives, wireless access points (routers), tablet computers, netbooks, chromebooks, smartphones and

smart devices, telephones, cellular telephones, personal digital assistants, pagers, MP3 players, wearable technology, any wireless communication device including emergency radios, and/or future technological innovations, whether accessed on or off site or through district-owned or personally owned equipment or devices, software, peripherals, accounts, passwords, ID numbers, student information systems, and any and all data, equipment, or electronic devices owned or leased by the District.

System administrator: A person employed by District whose responsibilities include system, site, or network administration. A system administrator performs functions including, but not limited to, installing hardware and software, managing computer networks, and keeping computers operational and investigating violations of the Agreement.

User: Someone who does not have system administrator responsibilities for computer resources or networks but who makes use of computer resources or networks. A user is still responsible for his or her use of the computer.

SECTION 3.
COMPUTER RESOURCES ACCESS AND EMPLOYEE RESPONSIBILITIES

Section 3.1 Access

District is committed to providing access to computer resources to all current employees and students consistent with the education and service missions of District. The District may place reasonable restrictions on the sites, material, information and/or data that employees may access through the system. The District reserves the right to suspend access at any time, without notice, for any reason.

Section 3.2 Privileges

3.2.1 Users do not own accounts on District computers. District owns the accounts and grants users the privilege of using the accounts.

3.2.2 Any District employee or student may apply for a user ID to utilize e-mail, Internet services and other computer resources offered by District. Such an application may be granted only if the applicant signs the Computer Use Agreement.

Section 3.3 Responsibilities

As a condition of maintaining the privilege of using District computer resources, each user will be held responsible for his or her own actions which affect such resources.

3.3.1 District computer resources are primarily to be used for District-related business, instruction, learning, and administrative activities. Use of District computer resources to engage in personal communications is not permitted, except for incidental personal use that does not interfere with District business and operations, the work productivity of any District employee, or compromise the safety and security of District computer resources.

3.3.2 Users shall not attempt to modify any system or network or attempt to "crash" or "hack" into District systems. Users shall not tamper with any software protections or restrictions placed on computer applications or files. Unless properly authorized, users shall not attempt to access restricted portions of any operating system or security software. Users shall not attempt to remove existing software or add their own personal software to District computers and systems unless authorized. Users shall not add personal network devices onto the district's network.

3.3.3 Users shall use only their own designated computer accounts. Users are required to keep all user ID's, passwords, and account information confidential, and shall take reasonable precautions to prevent others from obtaining this information. Accounts are not transferable, and users shall not allow others to use their accounts. Users may never share account login and password with students and users may never let students use a staff login. Users shall respect the privacy and personal rights of others, and are prohibited from accessing or copying another user's e-mail, data, or other files without the prior express consent of that user.

3.3.4 Users are responsible for using software and electronic materials in accordance with copyright and licensing restrictions. The copying of software that has not been placed in the public domain is expressly prohibited by the Agreement.

3.3.5 No Expectation of Privacy: District computer resources and all user accounts are the property of District. There is no right to privacy in the use of the computer resources or user accounts. All passwords created for or used on any District computer resources are the sole property of the District. The creation or use of a password by an employee on District computer resources does not create a reasonable expectation of privacy. The District reserves the right to monitor and record all use of District computer resources, including, but not limited to, access to the Internet or social media, communications sent or received from District computer resources and text messaging or instant messaging utilizing District computer resources.

In addition, users are hereby put on notice as to the lack of privacy afforded by electronic data storage and electronic mail in general, and must apply appropriate security to protect private and confidential information from unintended disclosure. Electronic data, including e-mail, which is transmitted through District computer resources is more analogous to an open postcard than to a letter in a sealed envelope.

District reserves the right to monitor and access information contained on its computer resources under various circumstances including, but not limited to, the following circumstances:

3.3.5.1 Under the California Public Records Act ("CPRA"), electronic files are treated in the same way as paper files. Public documents are subject to inspection through CPRA. In responding to a request for information under the CPRA, District may access and provide such data without the knowledge or consent of the user.

3.3.5.2 District will cooperate with any local, state, or federal officials investigating an alleged crime committed by any person who accesses District computer resources, and may release information to such officials without the knowledge or consent of the user.

3.3.5.3 The contents of electronic messages may be viewed by a system administrator in the course of routine maintenance, or by the system administrator, or designee(s) as needed for District administrative purposes, including investigation of possible violations of the Agreement or other District policies, and monitoring of on-line activities of minor students.

3.3.5.4 Electronic mail systems store messages in files. These files are copied to back-up tapes or other media in the course of system backups. The contents of these files and the copies on system backups are subject to disclosure as stated in the preceding paragraphs.

3.3.6 Receipt of Offensive Material: Due to the open and decentralized design of the Internet and networked computer systems, users are warned that they may occasionally receive materials which may be offensive to them. Users should report all such occurrences to the system administrator.

3.3.7 Records. Any electronically stored information generated or received by an employee which constitutes a District or student record shall be classified, retained and destroyed in accordance with the District's applicable records retention policies and procedures.

Section 3.4 Ethical Standards

All users must abide by ethical standards of on-line behavior that assure equitable, effective and efficient access and use of computer resources. Such ethical standards include, but are not limited to:

3.4.1 Honesty:

3.4.1.1 Users agree to represent themselves according to their true and accurate identities in all electronic messages, files and transactions at all times.

3.4.1.2 While using District computer resources, users agree to act within District standards of conduct including the prohibition on plagiarism.

3.4.2 Respecting Rights of Others:

3.4.2.1 Communicating in the same manner as is expected in the classroom or in the office (e.g., users should refrain from profanity and vulgarity). Users shall not use District computer resources in any unlawful manner including, but not limited to, attempting to defraud another person or entity, threatening harm to another person, procuring or distributing obscene material in any form, unlawfully harassing another person, or bully/cyber-bully any other person.

3.4.2.2 For purposes of the Agreement, "obscenity" or "obscene" means words, images or sounds which a reasonable person, applying contemporary community standards, when considering the contents as a whole, would conclude that they appeal to prurient sexual/physical interests or violently subordinating behavior rather than an intellectual or communicative purpose, and materials that, taken as a whole regarding their content and their particular usage or application, lack any redeeming literary, scientific, political, artistic or social value.

"Harassing" or "harass" means to engage in a knowing and willful course of conduct directed at another person which seriously alarms, annoys or harasses another person, and which serves no legitimate purpose. In addition, "Harassment" also means subjecting another person to unwelcome sexual advances, requests for sexual favors, and other verbal, visual or physical conduct of a sexual nature as set forth in California Education Code section 212.5.

"Bullying" and "cyber-bullying" are defined and governed by board policy BP 5131.2(a).

3.4.4 Users shall respect the integrity and content of electronic documents or records issued or posted on-line by employees or students.

3.4.5 Users shall have respect for the access and security procedures and systems established to ensure the security, integrity and operational functionality of District computer resources.

Section 3.5 Disclosure of Personal Information

Employees shall not disclose confidential student information through use of computer resources in a manner which violates either the California pupil privacy laws (Ed. Code § 49060 et. seq.) or the Federal Education Rights and Privacy Act ("FERPA") (20 U.S.C. § 1232g). Employees should not disclose personal information about themselves on the Internet or in e-mails as this information may be used by third parties to invade the privacy of the user.

SECTION 4.

APPROPRIATE AND INAPPROPRIATE USES

District computer resources exist to support the instructional, cultural, research, professional and administrative activities of the District community. In general, the same guidelines that apply to the use of all District facilities apply to the use of District computer resources. All users are required to behave in a responsible, ethical and legal manner as defined by the Agreement, and other existing District policies and regulations. The following sections define appropriate and inappropriate use of District computer resources:

Section 4.1 Appropriate Use

Activities deemed to be appropriate uses of District computer resources include the following:

4.1.1 Educational use (students)

Carrying out District course assignments and activities requiring access to and use of computer resources, including:

4.1.1.1 Authorized access to and use of computer programs licensed by District available on stand-alone and networked computing stations.

4.1.1.2 Authorized access to lab and campus networks to perform and complete required course work for District courses in which the user is currently enrolled.

4.1.1.3 Authorized access to District student e-mail accounts.

4.1.1.4 Authorized independent study and research.

Users agree to follow any computer use policies established by individual computing labs and network systems and to obey directives issued by authorized District personnel supervising such labs and systems.

4.1.2 Instructional use (teachers)

4.1.2.1 Classroom instruction.

4.1.2.2 Research connected to academic and instructional concerns and interests.

4.1.2.3 Communication with colleagues and professional organizations and institutions if such communications are related to District educational programs and activities.

4.1.3 Administrative use (administrators)

4.1.3.1 District administrative and business communications and transactions.

4.1.3.2 Communication with colleagues and professional organizations and institutions if such communications are related to the operation of District.

4.1.3.3 Research connected with District concerns and interests.

4.1.4 Request to unblock Internet site access by District employees

In the event that a District employee has a legitimate and job-related need to access material which is otherwise prohibited by the Agreement or cannot be accessed because of restrictions placed on the material by an Internet blocking or filtering measure, such employee may submit a written request to the Director of ITS or designee requesting permission to access specific sites for the purpose of completing such job-related tasks or research.

4.1.5 Personal Technology Use

District recognizes that the use of personal technology devices, which are not owned by the District, may be beneficial to both District employees and students. Personal devices such as laptops, PDAs, tablets, smartphones, memory sticks and other personal computing devices may be used by district staff in the course of their work at the district, provided that the device is protected by District approved and current and active security software, and that no student or pupil data is stored on the device. All Internet access to personal devices is provided through the district's Wi-Fi network. Personal devices may never be plugged into the district's wired network. The use of Personal devices with District computer resources, or through the district's Wi-Fi network, is subject to all terms and conditions of this Acceptable Use Policy. Personal devices will have limited access to district resources, and may be refused network access if the device appears unprotected by security software or if a signed Acceptable Use Policy is not on file. Similarly, no student/pupil data may be stored on an "off-campus" personal computing device such as a home PC or personal cell phone. Student personal device are subject to the same policies.

No Expectation of Privacy: When using District computer resources, through either a District device or personal device, employees do not have an expectation of privacy in anything they create, store, delete, send or receive through the District's computer resources, whether utilizing personal, password protected accounts or otherwise. Any use of a personal device to access District computer resources or conduct District business may subject the contents of the device and any communications sent or received on the device to disclosure pursuant to a lawful subpoena or public records request.

District employees may only use personal cell phones or other communication devices during non-duty times of the workday or for brief conversations. Instructional time may not be interrupted by a personal cellular telephone or mobile communication device, except in an emergency. Such activities shall not interfere with the work efficiency or performance of the employee and shall not interfere with the rights or work efficiency or performance of others. Access to district email on personal communication devices is allowed, subject to the limitations related to pupil data stated above.

Section 4.2 Inappropriate Use

Use of District computer resources for purposes other than those identified in Section 4.1 is not permitted. Users who violate this section of the Agreement by engaging in inappropriate use of District computer resources will be subject to restriction, suspension, or revocation of user privileges and may be subject to discipline and criminal or civil sanctions if permitted by law. Users are specifically prohibited from using District computer resources in any manner identified in this section.

4.2.1 Displaying, viewing, downloading, sending or otherwise accessing material that is obscene, pornographic, or harmful to minors. The District will utilize Internet filtering and/or blocking measures to attempt to prevent user access to such materials.

4.2.2 Using District computer resources for personal purposes, other than incidental use.

4.2.3 Destroying or damaging equipment, software, or data belonging to District or others.

4.2.4 Disrupting or unauthorized use of District accounts, access codes, or ID numbers.

4.2.5 Using District computer resources in ways which intentionally or unintentionally impede the computing activities of others are prohibited. Such activities include, but are not limited to: disrupting another person's use of computer resources by game playing, sending an excessive number of messages or e-mail, making or printing excessive copies of documents, files, data, or programs, introducing computer viruses onto District computer resources, or impersonating any person or entity under a false or unauthorized name.

4.2.6 Using District computer resources to violate copyrights, trademarks, and/or license agreements.

4.2.7 Using District computer resources to violate another person's privacy including, but not limited to, obtaining, accessing, distributing, or using another user's account, ID number, password, electronic files, data, e-mail, or confidential personal information.

4.2.8 Using District computer resources in an effort to violate District's academic policies.

4.2.9 Transmitting any advertising or promotional materials or engaging in commercial activity or political lobbying which is unrelated to District business including, but not limited to, buying, selling, advertising, or viewing property or services posted on ebay, Craigslist, Amazon, or other commercial websites.

4.2.10 Copying system files, utilities and applications that expressly belong to District without authorization.

4.2.11 Sending or storing messages and/or materials with the intent to defraud, harass, intimidate, defame, threaten, unlawfully discriminate, or otherwise violating the District's ethical standards under Section 3.4.

4.2.12 Mass mailing/emailing/texting, "spamming," or "mail bombing" directed to "All District Employees" or to any large subgroup of District employees shall be approved by the sender's immediate supervisor prior to being sent.

4.2.13 Disabling, tampering with, hacking or trying to break into any software protections or restrictions placed on computer applications or files.

4.2.14 Knowingly or carelessly introducing any invasive or destructive programs (e.g., spyware, viruses or worms) into District computer resources.

4.2.15 Attempting to circumvent local or network system security measures.

4.2.16 Installing unauthorized software programs on District computers or network systems and/or using such programs.

4.2.17 Ignoring or disobeying policies and procedures established for specific computer labs or network systems.

4.2.18 Using District computer resources for any activities which violate or are inconsistent with District policy or regulations.

4.2.19 Employees should not "friend" or "like" any students on Social Networks such as Facebook and MySpace using the employee's district email or credentials, or using district computer equipment. Should an employee choose to "friend" or "like" a student on any Social Network, it should be done on personal equipment using personal accounts outside the District.

4.2.20 Staff may only email students related to activities at the District, and if the student has a district email address, said district email address is the preferred email address to use in all staff-student email communication. Any non-district related staff-student communication should be carried out on personal equipment, using personal accounts outside the district.

4.2.21 Installing personal network devices, such as Wi-Fi access points, switches, VPNs, and routers, anywhere on the district network.

SECTION 5.

VIOLATIONS: REPORTING AND CONSEQUENCES

Section 5.1 Reporting Violations

5.1.1 Student Violations

Users shall report any suspected violation of the Agreement by a student to the Director of ITS or designee, who shall immediately refer the matter to the system administrator for review. The system administrator shall then determine whether a violation of the Agreement has occurred. If the system administrator determines that violation has occurred, the system administrator may restrict, suspend, or revoke the user's privileges. The user may also be subject to appropriate discipline.

5.1.2 Employee Violations

Users shall report any suspected violation of the Agreement by a District employee to the employee's supervisor who shall immediately refer the matter to the system administrator and the Assistant Superintendent of Human Resources for review. The Director of ITS and/or the Assistant Superintendent of Human Resources shall then determine whether a violation of the Agreement has occurred. If the Assistant Superintendent of Human Resources determines that a violation has occurred, he or she may take immediate action to restrict, suspend, or revoke the user's privileges. The user may also be subject to appropriate discipline.

ACCEPTABLE USE POLICY AND COMPUTER USE AGREEMENT DISTRICT EMPLOYEE

I have read the District's Acceptable Use Policy and Computer Use Agreement and understand its provisions. I accept responsibility for the appropriate use of District computer resources. I understand that use of computer resources in violation of the Agreement may result in the revocation or restriction of user privileges and appropriate discipline. I understand that there is no expectation of privacy when using District computer resources or when my personal device accesses District computer resources. I agree to report any use which is in violation of the Agreement to the system administrator or appropriate employee supervisor.

_____

Employee [PRINT NAME]

_____

Signature

_____

Date

School/Department

SIGN & DATE THE COMPUTER USE AGREEMENT

RETURN THIS PAGE TO YOUR SITE PRINCIPAL

OR DEPARTMENT SUPERVISOR