

## Personnel

Subject: Acceptable Use Policy

Section One: Purpose

The purpose of this Policy is to describe the expectations of the Lancaster Central School District (LCSD) for the acceptable use of its equipment, electronic media, and services, including computers, email, telephones, voicemail, fax machines, software, subscriptions, Internet, and to protect the security and integrity of Lancaster Central School District's (LCSD) data and technology infrastructure.

To better serve our students and provide our employees with the best tools to do their jobs, the LCSD makes available to our employees access to one or more forms of equipment, electronic media, and services. LCSD encourages the use of these media and associated services because they can make communication more efficient and effective, and because they are valuable sources of information. However, all employees and everyone connected with the District should remember that electronic media and services provided by the District are District property and their purpose is to facilitate and support District business. All computer users have the responsibility to use these resources in a professional, ethical, and lawful manner.

No policy can include rules to cover every possible situation. Instead, this policy is designed to express LCSD's philosophy and set forth general principles when using electronic media and services. The District's expectation of staff, students, and others is that they will access the District's computer systems for educational purposes in a polite, professional, and ethical fashion. Any violation of this policy, as determined by the District, will be addressed through the District's discipline procedures.

Section Two: Covered Individuals and Entities

This policy applies to all representatives of the District, which includes all employees, including all faculty and administration, contractors, vendors, affiliates, and other third-party partners with whom the District has a relationship, collectively referred to throughout this policy as "District Representatives." As we communicate electronically and, on the Internet, it is important to think of ourselves as representatives of the District.

Every District Representative will be required to sign (electronically) this Acceptable Use Policy on an annual basis. This form supersedes previous documents and forms. District Representatives who have signed previous forms must also complete this new form.

Section Three: Expectations for Acceptable Use

District Representatives are expected and encouraged to use the District's equipment, electronic media and services to achieve educational benefits for themselves and the students of the District. In the course

(Continued)

## Personnel

Subject: Acceptable Use Policy (Cont'd.)

of performing your duties for the District, you may use the District's equipment, electronic media, and services to communicate with others in the District and those outside the District on District business and to research topics applicable to District projects on which you are working. Internet access is provided to facilitate District related communications and to enhance your productivity. The Internet and the District's equipment, electronic media, and services are powerful tools for education. We expect that you will use the tools to expand the knowledge and understanding of all District Representatives and students.

Any and all documents, images, communications, information, emails, electronic data, and Internet data in any format that is composed, transmitted, downloaded, saved, or received on District equipment and/or via our computer communications systems is considered to be part of the official records of the District and, as such, is subject to inspection and/or disclosure to law enforcement or other third parties. The electronic communications systems owned, supplied, or funded by the District, including the Internet, email, voicemail, telephone, mobile devices, etc., should be used for legitimate educational purposes. Equipment (e.g., work stations, mobile devices) use and access will depend on your job functions. The contents of any communications transmitted through or stored within these systems/devices constitute District property and are subject to review by and disclosure to the District. Furthermore, in some situations (e.g., litigation involving the District or law enforcement matters) these communications may be subject to disclosure to a third party outside of the District.

In order to ensure that the systems are being used properly and in compliance with this Policy, the District may, without notice, periodically access, display, copy or listen to any messages or communications sent, received, created, or stored through or in its systems or in devices that the District owns, supplies, or funds, whether stored or in transit.

District Representatives have no expectation of privacy in files, removable media, email, voicemail, or documents that have been created in, entered in, stored in, downloaded from, or used on District equipment. Additionally, there shall be no expectation of privacy when using District services, such as Google Workspace, on non-district and/or personally owned devices. In particular, if utilizing a District service on a personally owned device, your use of that service (only your activity within that service) remains subject to inspection and review as needed. This does not mean that the entire contents of your personally owned device are subject to inspection and review, but that your activity within the District owned service only, e.g., sending emails with your District Google Workspace account or utilizing Google Classroom, may be reviewed and monitored. All District hardware, including computers and equipment, if the property of LCSD will fall under the guidelines listed in this Policy.

Your use of the District's equipment and systems constitutes your permission for the District to monitor communications and to access files/postings/data made on or with these tools, whether or not made/posted during your regular hours of work. The fact that a District Representative may be permitted to choose his/her own password does not imply that they have any justifiable privacy expectations in the material protected by password. There is no such privacy right and even personal information transmitted or stored on the District's equipment or network is subject to inspection at any time. All messages sent or received over District voicemail, the District Internet, personal devices supplied or funded by the District, or related District operations and/or information transmitted by or stored on District servers or District owned computers and equipment are subject to review by the District in its sole discretion.

(Continued)

## Personnel

## Subject: Acceptable Use Policy (Cont'd.)

District representatives are prohibited from using their District email address or other District supplied account credentials to register for access to 3rd party accounts and services, websites or non-District controlled applications unless requested by, required by, or approved by the District. Additionally, please note that all publicly displayed information on District equipment, even on social and professional networking sites, may be reviewed by the District.

District Representatives are responsible for the security of their equipment, files, and passwords. District Representatives shall not disclose their individual passwords to others or use others' passwords. This includes family and other household members when work is being done at home. District Representatives shall promptly notify their immediate supervisor of security problems. If the District Representative does not have an immediate supervisor or if their immediate supervisor is unavailable, the District Representative shall notify the Information Services Department. District Representatives with access to student records may not use, release, or share these records except as authorized by federal and state law. Security and confidentiality of records, reports, and files are matters of critical importance to the District. Each individual who has privileged access to sensitive, classified, or confidential data is expected to adhere to the security and confidentiality principles stated below.

## Examples of Unacceptable Use

- a. District Representatives shall not share their password with any person, or permit any other person to access information under their account;
- b. District Representatives shall not go beyond their authorized access to the District information services or other District equipment or software including the files or accounts of others;
- c. District Representatives shall not permit the unauthorized use of any information in documentation, configuration file, records, reports, and files which are accessed, processed, maintained, or stored by the Information Services Department;
- d. District Representatives shall not disclose the confidential contents of any record, report, or file to any person, except in the conduct of official work assignments;
- e. District Representatives shall not knowingly include a false, inaccurate, or misleading entry in any official non-test record, report, or file;
- f. District Representatives shall not change, copy, rename, delete, read or otherwise access files not created by the District Representative;

(Continued)

## Personnel

## Subject: Acceptable Use Policy (Cont'd.)

- g. District Representatives shall not use or acquire a password, access a file, or retrieve any stored communication without authorization;
- h. District Representatives shall not knowingly disrupt or attempt to damage or disrupt any computer, system, system performance, or data. This includes the introduction of malicious programs into the network or server;
- i. District Representatives shall not knowingly destroy data from any record, report, or file, except as authorized;
- j. District Representatives shall not seek personal benefit from or use information that they have acquired as a result of their access to data;
- k. District Representatives may not use LCSD equipment or computer network in any way which results in unauthorized charges or expenses to the District.
- l. District Representatives shall not use District equipment to engage in illegal acts; and
- m. District Representatives shall not knowingly cause or assist another person to violate these principles.

LCSD makes no warranties of any kind, whether express or implied, for services provided and is not responsible for any damages suffered while on the system including loss of data and inaccurate or poor-quality information obtained from the system. Users are responsible for backing up their data and saving files if so desired.

## Section Four: Staff Use of Mobile/Personal Electronic Devices

All staff members who use mobile electronic devices in the course of their job duties, including but not limited to laptop computers, tablets, mobile phones, flash drives, e-readers, scanners, printers, digital cameras, camcorders, when used in conjunction with the LCSD wireless network, shall abide by this policy section which governs the use of this type of equipment. Any mobile electronic device that runs software or systems including, but not limited to, Windows, macOS, Linux, ChromeOS, Android or iOS is considered a “computing device” for the purposes of this policy.

## Confidentiality and Private Information and Privacy Rights

Access to confidential data is a privilege afforded to LCSD staff in the performance of their duties. Safeguarding this data is a District responsibility that the Board of Education takes very seriously. Consequently, LCSD employment does not automatically guarantee the initial or ongoing ability to use mobile/personal electronic devices to access the District Computing System (“DCS”) and the information

(Continued)

## Personnel

Subject: Acceptable Use Policy (Cont'd.)

contained therein.

Confidential and/or private data, including but not limited to protected student records, employee personal identifying information, and LCSD assessment data, shall only be loaded, stored, or transferred to LCSD- owned electronic devices which have encryption and/or password protection. This restriction, designed to ensure data security, encompasses all computers and electronic devices within the DCS, any mobile devices, including flash or key drives, and any electronic devices that access the DCS from remote locations. Staff will not use email to transmit confidential files in order to work at home or another location. Staff will not use cloud-based storage services (such as Dropbox, Google Drive, Microsoft OneDrive, Apple iCloud, etc.) for confidential files.

Staff will not leave any electronic devices unattended with confidential information visible. All electronic devices are required to be locked down while the staff member steps away from the electronic device and settings enabled to freeze and lock after a set period of inactivity.

Staff data files and electronic storage areas shall remain LCSD property, subject to LCSD control and inspection. The Information Services Department may access all such files and communications without prior notice to ensure system integrity and that users are complying with requirements of this policy and accompanying regulations. Staff should not expect that the information stored on the DCS will be private.

#### Personal Electronic Devices

Staff may choose to use their own personal electronic devices to perform job-related functions, rather than the technology assigned to them by LCSD. If a staff member chooses to use a personal electronic device, the following guidelines will apply:

- 1) Use of any mobile electronic device during the school day, whether LCSD-issued or personal electronic device, should not interfere with the staff member's ability to carry out daily responsibilities.
- 2) The entire cost to acquire all personal electronic device services is the responsibility of the staff member. Services that may incur a financial cost to LCSD, such as phone options or other "apps" are not allowed. LCSD does not agree to pay such charges and staff who desire these options must assume all costs incurred for such charges.
- 3) LCSD shall not be liable for the loss, damage, misuse, or theft of any personal electronic device brought to school. Loss or damage to any personal electronic device is solely the responsibility of the staff member. In the event that a personal electronic device is lost, stolen, or damaged, LCSD is not responsible for any financial or data loss, except for incidents that are covered under Collective Bargaining Agreements.
- 4) Staff assumes complete responsibility for problem resolution of a malfunctioning personal electronic device or software contained on a personal electronic device, file formatting, repair, as well as any connectivity and technical issues that may arise with the personal electronic device.

(Continued)

## Personnel

Subject: Acceptable Use Policy (Cont'd.)

- 5) The LCSD Board of Education expressly prohibits use of any personal electronic devices in locker rooms, restrooms, health offices, pool areas, and any other areas where a person would reasonably expect some degree of personal privacy.
- 6) Personal electronic devices may not be connected to the network by a network cable plugged into a data outlet. Network access is provided via wireless access only. Access to any other LCSD network using a personal electronic device is prohibited.
- 7) Personal electronic devices must not be used to establish a wireless ad-hoc or peer-to-peer network while connected to LCSD's network. This includes, but is not limited to, using a personal electronic device as a cabled or wireless hotspot. Any staff member who violates the conditions of this regulation using a personal electronic device will have access privileges withdrawn.
- 8) LCSD reserves the right to monitor, inspect, and/or examine a staff member's District network activity if there is reasonable suspicion, as determined by the Superintendent or his/her designees, that school and/or LCSD policies or local, state, and/or federal laws have been violated. Searches will be limited to circumstances in which there is reasonable suspicion that the search will produce evidence of the suspected misconduct. If the District has such reasonable suspicion, the District will advise the staff member. The District will address any violation of this policy through the District's discipline procedures in accordance with applicable collective bargaining agreements and State and Federal law. When applicable, law enforcement agencies may be involved. (See Section Nine: Violations)

#### Section Five: District Internet Use Standards

Access to the Internet is provided for the benefit of the District and our students and mission. The Internet should be used in conjunction with the District's business and your job responsibilities. Each District Representative using the Internet is responsible for maintaining and enhancing the District's public image and for furthering and protecting the interests of the District and our students and mission. The Internet is a business tool which must be used in a productive manner.

All Internet usage on the District network is subject to District inspection. In addition, the District has the capability to obtain lists of websites (URLs) viewed by District Representatives, which may be monitored at any time without notice. You should be aware that our firewall and other security tools create an audit log detailing requests for access in either direction (outside of District to inside District and inside of District to outside) by each user. Each Internet user is responsible for the content of all text, audio, video, or image files sent or received by them over the Internet. Internet usage must comply with the District's policies regarding discrimination, harassment, student safety and welfare, social/business networking, blogging, and other Internet-based/web postings.

(Continued)

## Personnel

Subject: Acceptable Use Policy (Cont'd.)

Examples of Unacceptable Uses of the District Internet

- a) At a minimum, transmission of abusive, profane, obscene, fraudulent, sexually explicit, slanderous or libelous content is prohibited.
- b) No message may be sent, forwarded, shared, or otherwise disseminated if it could be construed as harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, disability, religious beliefs, political beliefs, or any other basis protected by law.
- c) The Internet cannot be used for knowingly transmitting, retrieving, or storing any communication (e.g., forwarded emails that contain jokes, pictures, downloading or transmitting of copyright material – such as music video and games, etc.) that is: (1) Discriminatory or harassing; (2) Derogatory to any individual or group; (3) Obscene, sexually explicit, or pornographic; (4) Defamatory or threatening; (5) In violation of any license governing the use of software; (6) In violation of any other law or rule; (7) Used for private/personal business purposes, product advertisement, or political lobbying; or (8) Engaged in for any purpose that is illegal or contrary to LCSD policy or District interests and/or reputation.
- d) Downloading of large files and/or other high-volume activities (i.e., video streaming, downloading/listening to music, use of peer-to-peer networking) is prohibited.
- e) Internet activities that consume inordinate amounts of bandwidth will be reviewed for approval by the Curriculum Director and Information Services Department.
- f) Personnel matters should never be discussed in public Internet spaces. All concerns about personnel matters should be addressed with the Superintendent or his designees. Issues regarding particular students should never be discussed in public Internet spaces.

Failure to adhere to this policy or the above Internet Use Standards will result in disciplinary action ranging from termination of Internet/equipment access to termination of employment.

Section Six: Social Media Standards

It is the District Representative's responsibility to protect and further the District's values and mission. This includes all dealings with students, professionals, or the public. The District's personnel policies detail the District's expectations and your responsibilities as a District Representative; however, the advent of computer networking, personal websites, web logs, blogs, and other social and business conversational media, as well as other uses of technology (e.g., text messaging, wikis), have increased our exposure and the risks to our reputation. For this reason, the District has developed these standards for behavior in virtual public forums.

(Continued)

## Personnel

## Subject: Acceptable Use Policy (Cont'd.)

If you choose to post on a personal website, or to participate in social/business networking, web- groups, blogs, or chat groups, whether during business hours or while off duty, you should adhere to the following points and policies:

## Personal Networking

The District understands that District Representatives may maintain or contribute to personal blogs, message boards, conversation pages, and other forms of social/conversational media, including photo/video posting sites, outside of their job function and may periodically post information about their life, which may include their job. The following rules must be followed:

- a) If a District Representative posts job-related information, they are required to abide by the District's policies.
- b) The District cannot be identified or identifiable in any such personal posting. Please keep in mind that many District Representatives are well-known in their communities and any posting may be viewed as connected to the District.
- c) If a District Representative is engaging in any communication on external social media platforms personally, they should not use the District's name or identifying attribute in their username, or screen name, nor should they speak as a representative of the District.
- d) If a social media profile identifies the District in any way, or if the District could be connected to the profile, it is the District Representative's responsibility to ensure their comments and all content posted are appropriate, respectful, and professional.
- e) District Representatives should not post or allow others to post to their social media website statements or images that could be deemed harmful to the District's reputation or in violation of District policies/the law.
- f) No District Representative may make comments or statements on any online forum which discriminate, attack, threaten, or otherwise harm any other District Representative or student.

## Business Networking

District Representatives may not establish social/conversational media sites representing District programs and services without permission from the Superintendent or his designee.

- a) No District Representative may host or maintain a blog, vlog, posting, website, etc. using the District's technology or equipment if it relates or reflects upon the District.

(Continued)

## Personnel

Subject: Acceptable Use Policy (Cont'd.)

- b) The use of photos, logos, or images of the District, its students, or programs is prohibited without express advanced permission from the Superintendent or his designee. The District's intellectual property, such as logos, graphics, and copyrights may not be used in any manner for personal postings but may be used in certain business postings. In order to obtain advanced permission for the use of the District's intellectual property, you must contact the Superintendent or his designee.
- c) If you use the District's name for business networking purposes or make the District identifiable in any manner, you should be especially careful to support the District's image and mission/purpose.

General Policies Applicable to both Personal and Business Networking

- a) District Representatives should be aware of and comply with codes of conduct outlined in the LCSD Employee Handbook and other District policies or agreements.
- b) District Representatives may not disclose confidential information, including any information about a student, project, or personnel matter/issue.
- c) District Representatives may not disclose proprietary information.
- d) District Representatives may not use postings as a mechanism to harass or otherwise harm other District Representatives or make comments or statements or take any action in any online forum which discriminates against, attacks, threatens, or otherwise harms any other District Representative, student, or community member.
- e) Your communications online may be seen by others as a reflection or representation of your character, judgment, and values, and in some instances may be perceived by others as an indirect extension of the District, regardless of your intent. Posting some types of information may jeopardize your image and reputation and, by extension, the District's image and reputation.
- f) Information you share online may be posted in perpetuity, may be impossible to retrieve or eradicate, and may be forwarded or endlessly shared. Be especially careful when posting photographs, images, or personal information.
- g) All of the District's policies regarding confidential information apply to electronic information (e.g., Internet communications, Internet/network postings). No District Representative may reveal any information relating to the District's students or reveal internal District information on line or through electronic means without the prior permission of the Superintendent.

(Continued)

## Personnel

Subject: Acceptable Use Policy (Cont'd.)

- h) District Representatives may not make disparaging or inappropriate comments or statements about the District that do not align with the goals and mission of the District that are not protected under current labor law.
- i) All District Representatives will immediately cooperate with District management in removing any Internet data or postings that the District, if found through an investigation, deems violations of this policy.

#### Use of Social Media Websites

No District business may ever be conducted or shared on personal forums, blogs, personal email, or like accounts, unless it is within your job duties to post on such sites, after discussion with your immediate supervisor, and such immediate supervisor must first obtain approval from the Director of Instructional Technology Services and Accountability. Only official District accounts may be used by authorized District employees to conduct communications via social networks. Furthermore, and as consistent with this policy, personal conduct and postings on social networks must remain professionally appropriate when the District is referenced, identified or identifiable.

#### Reporting Abuse

Do not underestimate the power and speed of social media. Irreparable damage can result from certain postings in very short time frames, so it may be imperative that the District take immediate action with respect to violations of this policy. The District will investigate inappropriate usage and will respond to complaints made about posting/sites in violation of District policies.

If any District Representative becomes aware of any online posting that is in violation of this policy or other District policies, the District Representative must share that information with their Principal, Director of Elementary or Secondary Education, Director of Instructional Technology Services and Accountability, Information Services Manager, or the Superintendent. Failure to report known abuse may constitute grounds for discipline.

#### Media Inquiries

When representing the District, all media inquiries, including online media and bloggers, must be referred to the Director of Communications or the Superintendent before any comments are made.

Failure to adhere to this policy or the above standards will result in disciplinary action ranging from termination of Internet/equipment privileges to termination of employment.

(Continued)

## Personnel

Subject: Acceptable Use Policy (Cont'd.)

### Section Seven: Electronic Mail ("Email") Standards

Electronic mail, or email, is a valuable business communication tool, and users shall use this tool in a responsible, effective, and lawful manner. Every District Representative has a responsibility to maintain the District's image and reputation, to be knowledgeable about the inherent risks associated with email usage, and to avoid placing the District at risk. Although email seems to be less formal than other written communication, the same laws and business record requirements apply. Signature files should be limited to professional information. Graphic images (other than LCSD logo) and animations are prohibited. All email communications should be written in the style and manner, including grammar and proper decorum that you would employ in sending hard copy communications. You should not put anything in an email that you would not put in a formal letter.

It is important for all District Representatives to remember that although email is convenient, email is not a mechanism for communicating to all staff. We should use "Reply to All" messages sparingly and only when necessary, and avoid sending unnecessary attachments. Verify recipients before sending an email.

Email, when sent or received on the District network and/or equipment, shall not be considered private. In addition, the superintendent (or his/her designee) has the right of access to all email sent or received to District email addresses regardless of its origin. In the event of LCSD being involved in any legal proceedings, any relevant emails may have to be disclosed. Every user is responsible for all email originating from their user ID (email address). If you choose to use District WiFi with your personal email, that email is not private.

#### Examples of Unacceptable Uses of District Email

- a) Email may never be used to conduct job searches, post personal information to bulletin boards, blogs, chat groups, and list services, etc.
- b) Email may never be used for solicitation purposes.
- c) Attempts to read, delete, copy or modify the email of other users are prohibited.
- d) Forwarding of chain letters, pyramid messages, or similar schemes is not allowed.
- e) Forgery or attempted forgery of email is prohibited.
- f) Personnel matters should never be discussed through group emails. All concerns regarding personnel matters should be addressed with the Superintendent or his designee.
- g) Issues regarding particular students should never be discussed through group emails.

(Continued)

## Personnel

Subject: Acceptable Use Policy (Cont'd.)

Classified and Confidential

District employees and authorized users may NOT:

- a) Provide lists or information about District employees or students to others and/or classified information without approval. Questions regarding usage and requests for such lists or information should be directed to a Principal/Supervisor.
- b) Forward emails with confidential, sensitive, or secure information without Principal/Supervisor authorization. Additional precautions, such as encryption, should be taken when sending documents of a confidential nature.
- c) Use file names that may disclose confidential information. Confidential files should be password protected and encrypted. File protection passwords shall not be communicated via email correspondence.
- d) Use email to transmit any individual's protective personal information (PPI). PPI may include but not be limited to social security number, driver's license number or non-driver ID number, account number, credit/debit card number and security code, or any access code/password that permits access to financial accounts or protected student records.
- e) Send or forward email with comments or statements about the District that may negatively impact it.
- f) Send or forward email that contains confidential information subject to Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA), Education Law Section 2-D (EdLaw 2-D) and other applicable laws.

Failure to adhere to this policy or the above standards will result in disciplinary action ranging from termination of Internet/equipment privileges to termination of employment.

Section Eight: Expectations for Student Supervision

Employees who supervise students with access to technical resources shall be familiar with the LCSD Student Internet Use Agreement and enforce its provisions. Staff members who supervise students, control electronic equipment, or otherwise have occasion to observe student use of said equipment online shall make reasonable efforts to monitor the use of this equipment to assure that it conforms to the mission and goals of the LCSD.

Students are held to the same standards of good behavior whether they are using school computer networks or other electronic media or communications, including a student's own personal technology or electronic device while on school grounds or at school events. General rules for behavior and communication apply.

(Continued)

## Personnel

Subject: Acceptable Use Policy (Cont'd.)

Employees shall not assist a student to violate District policy and/or regulation, or fail to report knowledge of any student violations of the District's policy and regulation on student use of computerized information resources.

#### Section Nine: Violations

In addition to the general requirements of acceptable employee behavior, use which violates any other aspect of LCSD policy or regulations, as well as local, state, or federal laws or regulations is prohibited.

The Information Services Manager will report inappropriate behavior to the District Representative's Supervisor who will take appropriate disciplinary action. Any other reports of inappropriate behavior, violations, or complaints will be routed to the District Representative's Supervisor for appropriate actions.

District Representatives who engage in unacceptable use shall lose access to the District's computer system and may be subject to further discipline. The District will address any violation of this policy through the District's discipline procedures in accordance with applicable collective bargaining agreements and state and federal law. When applicable, law enforcement agencies may be involved. Corrective action may include termination of employment or relations/contract with the District, legal action, and criminal liability.

#### Employee Agreement on Use of District Technology Devices, Network, Email, and the Internet

I have read, understand, and agree to comply with the foregoing policies, rules, and conditions governing the use of the District's electronic communications equipment and services. I understand that I have no expectation of privacy when I use any of the equipment, electronic media, or services provided by the District. I am aware that violations of these guidelines on appropriate use of the systems and services may subject me to disciplinary action, including termination from employment or relation/contract with the District, legal action, and criminal liability. I further understand that my use of the District email and Internet may reflect on the image of LCSD and that I have the responsibility to maintain a positive representation of the District. Furthermore, I understand that this policy may be amended at any time and I am responsible for complying with this policy at all times.

My use of District equipment and resources, as well as return of this sign-off page, constitutes my further permission to allow the District to monitor, inspect, and/or intercept all materials/files/information described above, whether stored or in transmission. The District will not access my personal electronic devices or control my protected speech except as provided herein with respect to District-supplied or funded equipment or systems. However, absent my signature, my use of the District's equipment or equipment funded by the District, or my mention of the District in any communication which violates this policy, constitutes my permission for the District to monitor, inspect, duplicate, etc., my electronic communication.

(Continued)

Subject: Acceptable Use Policy (Cont'd.)

Employee Handbook

I have read and understand the LCSD Acceptable Use Policy and the Employee Handbook. I understand that violation of this Agreement may be grounds for disciplinary action, including termination.

Employee Signature/Date

Employee Print Full Name Legibly