ACCEPTABLE USE OF TECHNOLOGY AND ELECTRONIC INFORMATION RESOURCES

A. Applicability

This Board Policy applies to the use of all District owned, leased, or managed technology equipment, including but not limited to, computers, scanners, multifunction printers, fax machines, printers, telephones, cellular and smart phones, tablets, personal digital assistants, digital readers, pagers, MP3 players, USB devices, or any wireless communication device, and all associated software and firmware. Also included are all on-line services provided by the District including but not limited to, email accounts, Internet sites maintained for or by the District, logins, passwords, data, files, Internet access, voice mail, all business applications, and information transmitted by, received from, entered into, or stored in these systems (hereinafter “District Technology” or “Technology”).

This Board Policy applies to all District employees, including full-time, part-time and temporary, and to consultants who have access to District Technology. It applies equally to any remote or off-site use of District Technology.

B. Introduction

The Governing Board recognizes that technological resources can enhance employee performance by improving access to and exchange of information; 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 for purposes related to their employment. Personal activities will be limited and will in no way interfere with the educational/professional use for which hardware and software are intended, or with the efficiency or safety of the District’s resources, uses that are described as “unacceptable” must be avoided. Incidental personal use does not extend to family members or other acquaintances.

ACCEPTABLE USE OF TECHNOLOGY AND ELECTRONIC INFORMATION RESOURCES (continued)

The purpose of this Board Policy is to secure District Technology in a reasonable and economical manner against unauthorized access, use or abuse, while at the same time making such Technology accessible to authorized users for legitimate business and educational purposes.

C. Definitions

"Technology" includes, but is not limited to, computers, tablets, the Internet, telephones, cellular telephones, personal digital assistants, digital readers, pagers, MP3 players, iPod's, USB drives, wireless access points (routers), or any wireless communication device.

"District Technology" is that which is owned or provided by the District.

"Personal Technology" is non-District Technology.

D. Use of District Technology

Employees shall be responsible for the appropriate use of District Technology and shall use District Technology primarily for purposes related to their employment. Employees may use District Technology for incidental personal purposes provided that such use does not directly or indirectly:

- Interfere with District operations
- Interfere with the employee's or co-workers' employment or other obligations to the District
- Burden the District with noticeable incremental costs
- Involve sending regular or voluminous personal messages via lengthy email lists
- Create a hostile working or educational environment (including sexual or other forms of harassment)
- Violate any District policy or law, including obscenity laws.

E. Use of Personal Technology

The use of Personal Technology is subject to certain restrictions as set forth below.

F. Consequences for Violations of This Policy

Technology shall be used in a professional manner and may not be used in a manner that is inconsistent with any District Policy. Employees shall adhere to all security and other guidelines established by the District.

ACCEPTABLE USE OF TECHNOLOGY AND ELECTRONIC INFORMATION RESOURCES (continued)

Violations of the law or this policy may be reported to law enforcement agencies. In addition, violations of this policy may result in revocation (temporary or permanent) of user access and/or discipline, up to and including termination of employment, in accordance with District policies. Employees shall adhere to all applicable local, state, federal, and international laws relating to the access and use of computer systems, software and online services. The District will cooperate fully with appropriate authorities to provide information related to actual or suspected activity not consistent with the law.

G. No Expectation of Privacy

Employees shall have no expectation of privacy in any message, file, data, document, facsimile, or any other form of information accessed, transmitted to, received from, or stored on any Technology owned, leased, used, maintained, moderated, or otherwise operated by the District, including but not limited to, emails and other electronic communications. During the course of carrying out their responsibilities, authorized District personnel or other authorized representatives may access any Technology, including employee emails and other electronic communications without the knowledge of the user. The District also has software and systems in place that monitor and record all Internet/Intranet and email usage. The District may capture user activity such as network resource and file access, data created, sorted, or transmitted in any form, telephone numbers dialed and web sites visited. The lack of privacy expectation with regard to District Technology does not extend to a personal device owned by the individual employee except insofar as the employee uses that device to access the District network.

The use, creation or change of any password, code or any method of encryption or the capacity to delete or purge files or messages, whether or not authorized by the District, does not create any expectation of privacy in any message, file, data, document, communication, facsimile, or other form of information transmitted to, received from, or stored on any Technology.

Employees should not expect privacy in the contents of their personal files on the District's Internet system or other District Technology, including but not limited to emails, text messages and voicemail. District Technology is under the control of system administrators or managers who may access user files or suspend services on the systems they manage without notice as required to protect the integrity of computer systems or to examine accounts that are suspected of unauthorized use or of having been misused, corrupted or damaged.

In the performance of their duties, system administrators regularly monitor transmissions for the purpose of ensuring the proper functioning, reliability, and security of District Technology. During this process, they may observe certain transactional information and

the contents of electronic communications. System administrators who inadvertently discover or suspect improper activity in violation of law or policy are required to report such information to their supervisor.

Employees are advised that employee emails and other electronic communications pertaining to the business of the District generally are deemed to be public records and must be disclosed to members of the public upon request unless the records are specifically exempt from disclosure under the California Public Records Act. Moreover, documents may be subject to disclosure by subpoena or other legal process.

H. Filtering

In compliance with the Children's Internet Protection Act, 47 U.S.C. 254, the Superintendent or designee shall ensure that all District computers with Internet access have a technology protection measure that blocks or filters Internet access to visual depictions that are obscene, child pornography, or harmful to minors as defined in 47 U.S.C. 254 and that the operation of such measures is enforced. 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.

I. Confidentiality Obligations

The District endeavors to maintain the confidentiality of its internal email system and other electronically stored information and employees are expected to respect that confidentiality. Employees shall not copy, move, or otherwise transfer confidential or sensitive information or data to a directory or storage location that does not have adequate access restrictions. Employees are cautioned to follow all applicable laws and District policies in releasing student or personnel information electronically or otherwise. Disclosure of such information is generally prohibited. Employees shall not allow students to access employee accounts, passwords, grading programs or other restricted resources.

The District websites available to the general public must contain a Privacy Statement.

To safeguard and protect the proprietary, confidential, and sensitive business information of the District and to ensure that the use of all Technology is consistent with District legitimate business and educational interests, authorized representative of the District may monitor the use of Technology, messages, and files.

Users who become aware of a possible security breach involving the District Technology or data shall immediately notify the Director of Technology or the Superintendent's Office.

ACCEPTABLE USE OF TECHNOLOGY AND ELECTRONIC INFORMATION RESOURCES (continued)

J. Installation/Modification of Technology

Employees may not install or modify any software on District Technology without prior authorization from their supervisor and the Director of Technology. Software downloaded on District Technology must have a direct business use and must be properly licensed and registered. Users shall follow all published standards for workstation software.

Employees are not permitted to modify existing hardware or connect personal computers or equipment to the District's computer network without prior authorization from the Director of Technology. For example, employees are not permitted to connect personal cell phones or smart phones to the District's computers or networks without prior authorization.

K. The Superintendent or designee shall establish administrative regulations and an Acceptable Use Acknowledgement which outline employee obligations and responsibilities related to the use of District Technology. The Superintendent or designee shall provide copies of related policies, regulations, and guidelines to all employees who use District Technology. Employees shall be required to acknowledge in writing that they have read and understand the District's policies, regulations and guidelines.

L. Unacceptable Uses

The following use of District Technology is unacceptable and in violation of this Board Policy:

1. Activities that violate any federal, state, or local law or District Policy.

2. Downloading or distrusting non-licensed software or additional copies of licensed software that exceed the number licensed by the District. Copyrighted information or software for which the District does not have specific approval to store and/or use must not be stored on District Technology.

3. Propagating computer viruses.

4. Downloading, displaying, soliciting, archiving, storing, distributing, editing, or recording sexually explicit messages or images, including but not limited to, pornography or other visual depictions that are harmful to minors as defined in the Children's Internet Protection Act, 47 U.S.C. 254.

5. Downloading entertainment software of games, except as may be directly related to an employee's job duties (e.g., instructional materials).

ACCEPTABLE USE OF TECHNOLOGY AND ELECTRONIC INFORMATION RESOURCES (continued)

6. Downloading or installing any Internet/Intranet screen saver programs.

7. Disseminating printing, or sharing copyrighted materials, including articles and software in violation of copyright laws.

8. Operating a business or soliciting money for personal gain. Using District Technology for any activity that is commercial in nature not related to work at the District, such as consulting services, typing services, developing software for sale, advertising products, and/or other commercial enterprises for personal financial gain. Non-District personal solicitations are prohibited.

9. Using District Technology to defame or act abusively toward others or to provoke a violent reaction, such as stalking, acts of bigotry, threats of violence, or other hostile or intimidating "fighting words." Offensive or harassing statements or language, including disparagement of others based on their race, color, ethnicity, religion, national origin, veteran status, ancestry, disability, age, sex, sexual orientation, or other protected characteristic.

10. Gambling or engaging in any other activity in violation of local, state, or federal law.

11. Accessing or viewing information that promotes terrorism, espionage, theft or illegal drugs except in the course of legitimate research.

12. Making threats against any person or persons or engaging in any type of terrorist activity.

13. Urging the support or defeat of a political candidate or ballot proposition.

14. Disseminating, posting, or otherwise making available confidential, sensitive, or private information pertaining to students or employees to individuals who are not legally authorized to receive the information. Sensitive District material transmitted over the Internet (with authorization) shall be encrypted.

15. Disseminating defamatory information.

ACCEPTABLE USE OF TECHNOLOGY AND ELECTRONIC INFORMATION RESOURCES (continued)

16. Unnecessary or unauthorized Technology usage that causes or attempts to cause, damage to or interference with any Technology, network or server, either locally or on any network that disrupts the instructional or work environment. Knowingly running, installing or giving to another user, any program on any computer system or network with the intended purpose of damaging or placing excessive load on a computer system or network used by others. Performing an act without authorization that will interfere with the normal operation of District Technology. Disguising, misrepresenting, or concealing the identity of a computer system connected to the District network. Attempting to circumvent data protection schemes or uncover security loopholes without prior written consent of the appropriate authority.

17. Attempting to monitor or tamper with another user's electronic communications or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the user, except as otherwise permitted under this Board Policy.

18. Using or assisting another to use an account or obtain a password without appropriate authorization.

19. Employing, either directly or by implication, a false identity when using an account or other electronic resource or posting or sending an anonymous communication. This includes sending unauthorized mail that appears to come from someone else as well as posting or otherwise disseminating materials which misrepresent the identity of the sender.

20. Providing students with access to confidential materials, including but not limited to grades, archives, test materials, or other inappropriate information.

21. Streaming video or audio content for purposes other than legitimate District business or instructional purposes.

22. Posting on electronic bulletin boards, Web pages, or any other computer network-based dissemination channel, any materials that violate District Policy or codes of conduct.

23. Using District networks to gain, or attempt to gain, unauthorized access to any computer system.

24. Facilitating or allowing use of a computer account, password, and/or network access or resources by any unauthorized person.

ACCEPTABLE USE OF TECHNOLOGY AND ELECTRONIC INFORMATION RESOURCES (continued)

25. Posting an anonymous message or using web-based proxies/anonymizers or software that attempts to make online activity untraceable.

26. Sending emails or information that disrupts the instructional or work environment.

M. Web pages/Web 2.0 Sites

a. Access to Social Networking Sites

An employee with a school or District-related need to access a social networking site using District Technology must request such access from the Superintendent or designee. All postings to the site shall be business-related and consistent with Board Policy and Administrative Regulations.

b. Creation of School-Related Webpages/Web 2.0 Sites

- Definition of Web 2.0 site: A Web 2.0 site allows its users to interact with other users or to change website content, in contrast to non-interactive websites where users are limited to the passive viewing of information that is provided to them.

- Employees who wish to create a school or District-related webpage, either interactive (Web 2.0) or non-interactive, must have approval from the Superintendent or designee. The Superintendent or designee will approve the content of the site and determine whether the site will be structured to accept postings from individuals outside of the District. All such sites must be in compliance with the District's Board Policies.

- In determining whether to accept postings from individuals outside of the District for a particular purpose, the Superintendent may want to consult with legal counsel to determine the nature of the forum that is being created, as well as the ability of the District to exclude certain types of materials from the site without violating the free speech rights of the poster.

- If the Superintendent or designee approves the creation of a "limited public forum," (i.e., a site restricted to certain groups or dedicated solely to the discussion of certain subjects), any restrictions on speech shall be reasonable and viewpoint-neutral. The Superintendent or designee shall be responsible for monitoring the postings to the site and upon receipt of a complaint concerning inappropriate content shall take appropriate action. The site

should direct visitors to make complaints to the Superintendent or School Principal. The following types of postings shall be removed immediately: obscenity, pornography/child pornography, material that is harmful to minors as defined in 47 U.S.C. 254, material that constitutes or advocates illegal activity, material that discloses confidential information concerning District students or personnel, material that promotes the use of alcohol, tobacco or illegal drugs, material that advocates violence, hate groups or other dangerous groups, threats, material that discriminates against people based on a protected characteristic, materials that violate copyright laws, commercial advertising, defamatory information, private information concerning another person, including photographs, posted without that person's permission, material that urges the support or defeat of a political candidate or ballot proposition.

- Employees shall not permit students to access District computers that contain a Web 2.0 site unless the site is created specifically for the class and is monitored by the teacher to remove the types of materials listed in subsection above. All students assigned to the class (and their parents) must be able to access class-related sites developed and maintained using District or Personal Technology; other individuals shall be excluded from such sites. Teachers and others may not post student names, photographs, or work without prior written authorization from the student's parent or guardian.

c. Student Access to Employees' Personal Social Media Sites

- Employees are encouraged to carefully consider issues that may arise if they allow students to access their social media sites. For example, some parents perceive such access to be unprofessional. In addition, if students are engaging with each other on the site, the employee may have an obligation to monitor the communications for bullying or other inappropriate conduct. If an employee chooses to permit students to access their social media sites, it is recommended that all students in the class and all parents have such access. Employees are reminded that such sites should be professional and appropriate for students. It is suggested that employees maintain a separate social media presence for school/student use as opposed to the social media presence they have for their personal use.

- Social media sites that are accessible to District students or parents must include a disclaimer indicating that the site is not affiliated in any way with the District and the District does not endorse the contents of the site.

ACCEPTABLE USE OF TECHNOLOGY AND ELECTRONIC INFORMATION RESOURCES (continued)

N. Intellectual Property

Technology may provide access to material protected by copyright, trademark, patent, trade secrets, and/or export law. Employees may not assume that merely because information is available on Technology to which they have access that it may be downloaded or further disseminated.

Employees must ensure that use of any material from Technology will not violate applicable law or intellectual property rights of any third party. Employees who are unsure as to whether the downloading or use of such material violates the rights of a third party or applicable law should make no use of such material (including downloading it) until receiving appropriate approval from the owner of the intellectual property. Likewise, no District proprietary information, or any material protected by copyright, trademark, patent, trade secrets and export law may be copied, posted, or otherwise distributed without the express written permission of the District.

Employees who need information concerning copyright are directed to consult with the Director of Technology and/or appropriate resources, such as http://www.copyright.gov/ and Copyright Law in Cyberspace as indicated in the following website address: http://www.utsystem.edu/OGC/IntellectualProperty;distance.him.

O. Passwords

Employees are responsible for their passwords. Users may change generic passwords to personalized passwords and keep them secure. Continued use of a generic password can result in someone else sending messages in the owner's name, in which case, the owner is held responsible. Current passwords may be requested by an Employee's supervisor and the supervisor will take reasonable precautions to maintain the confidentiality of the password except as needed for legitimate business purposes as set forth in this Board Policy.

Employees shall not develop any classroom or work-related web sites, blogs, forums, or similar online communications representing the District or using District equipment or resources without permission of the Superintendent or designee. Such sites shall be subject to rules and guidelines established for District online publishing activities including, but not limited to, copyright laws, privacy rights, and prohibitions against obscene, libelous, and slanderous content. Because of the unfiltered nature of blogs, any such site shall include a disclaimer that the District is not responsible for the content of the messages. The District retains the right to delete material on any such online communications.

ACCEPTABLE USE OF TECHNOLOGY AND ELECTRONIC INFORMATION RESOURCES (continued)

The Superintendent or designee shall establish administrative regulations and an Acceptable Use Agreement which outline employee obligations and responsibilities related to the use of District technology. He/she 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.

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 acknowledge in writing that they have read and understood the District's Acceptable Use Agreement.

Use of Cellular Phone or Mobile Communications Devices

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. While on duty, an employee shall not use a cellular phone or other mobile communications device while driving except to make an emergency call to a law enforcement agency, a medical provider, the fire department, or other emergency services agency.

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

P. Internet Services

Employees shall not direct students to sign up for Internet services, such as e-mail accounts, without District authorization. Written permission from the parent/guardian shall be required in a form prescribed by the District.

Q. Digital Millennium Copyright Act (DMCA) compliance

The District shall take all actions necessary to comply with the DMCA service provider requirements, including but not limited to, taking down allegedly infringing material upon receiving notice from an aggrieved copyright owner or his representative; terminating access to individuals who are repeat infringers; and accommodating standard technical measures used by copyright owners to identify or protect copyrighted works as required by law. The Designated Agent for receiving notice of claimed infringement is the Superintendent or Director of Technology. In order to constitute effective notice of claimed infringement, a written communication must be received by the Designated agent that includes the following six elements or substantially complies with the following:

ACCEPTABLE USE OF TECHNOLOGY AND ELECTRONIC INFORMATION RESOURCES (continued)

a. A physical or electronic signature of the copyright owner or his authorized agent ("the complaining party")
b. Identification of the work claimed to have been infringed, or, if multiple copyrighted works are involved, a representative list of such works
c. Identification of the material to be removed or access to which is to be disabled, with information reasonably sufficient to permit the service provider to locate this content
d. Information reasonably sufficient to permit the service provider to contact the complainant party, such as an address, telephone number, and, if available, an email address
e. A statement that the complaining party has a good faith belief that display of the material in the manner used is not authorized by the copyright owner, its agent, or the law
f. A statement that the information in the notice is accurate, and under penalty of perjury, that the complaining part is authorized to act to protect an exclusive right that has allegedly been infringed

The District will promptly notify the individual who posted the allegedly infringing content that it has removed or disabled access to the content. This individual may then serve a counter-notification on the District. If the notice complies with statutory requirements, the District will re-post the material as required by law.

R. Endorsements or Hyperlinks

Unless authorized as stated herein, no person shall use the name "Lowell Joint School District" to imply, indicate or otherwise suggest that any corporation, firm, partnership, association, group, activity, or enterprise is connected or affiliated with, or is endorsed, favored, or supported by, or is opposed by the Lowell Joint School District. Use of the name "Lowell Joint School District," as well as hyperlinks to outside websites, may be approved by the Superintendent or designee if it is determined that such use is in the District's best interest; such approval shall be in writing.

S. Inadvertent Access

Employees who mistakenly access prohibited information or otherwise violate this Board Policy should immediately report the matter to their supervisor. This may help protect employees defend against a claim that they have intentionally violated District Policy.

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
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:
WEB SITES
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

Policy Adopted: November 5, 2007
Policy Revised: June 18, 2012; June 18, 2013