Delano Joint Union High School District

Administrative Regulation 4040
Employee Use of Technology

The District recognizes that electronic information resources can enhance productivity, facilitate professional communication, and assist in providing quality educational programs. This Policy applies to and describes the responsibilities and obligations of all employees using the District's electronic information resources, including computers, electronic devices, and network, and portions of this Policy also apply to an employee's personal computer and electronic device under certain circumstances, as described in the section on appropriate use of personal computers and devices.

DEFINITIONS

1. Definition of Electronic Information Resources

   The term "electronic information resources" ("EIR") includes District computers, electronic devices, and the District's electronic network.

2. Definition of District Electronic Record

   The term "District electronic record" means any writing containing information relating to any aspect of the business of the District, regardless of the writing's physical form or characteristics. For this purpose, "writing" means any handwriting, typewriting, printing, photostating, photographing, photocopying, transmitting by electronic mail or facsimile, and every other means of recording upon any tangible thing any form of communication or representation, including letters, words, pictures, sounds, or symbols, or combinations thereof, and any record thereby created, regardless of the manner in which the record has been stored.

3. Definition of Computer

   The term "computer" means any computer, including a laptop or notebook, whether or not the computer is equipped with a modem or communication peripheral capable of digital connection. The term "District computer" means

any computer that is owned, leased, or rented by the District, purchased with funds from a grant approved by or awarded to the District, or borrowed by or donated to the District from another agency, company or entity, whether or not the computer is equipped with a modem or communication peripheral capable of digital connection.

4. Definition of Electronic Device

The term "electronic device" means any device other than a computer that is capable of transmitting, receiving, or storing digital media, whether or not the electronic device is portable and whether or not the electronic device is equipped with a modem or other communication peripheral capable of digital connection. Electronic devices include, but are not limited to the following:

- Telephones
- Cellphones, including "smartphones"
- Radios
- Pagers
- Digital cameras
- Personal digital assistants, including but not limited to Blackberries, Palm Pilots, and "smartphones"
- Portable storage devices, including but not limited to thumb drives and zip drives
- Portable media devices, including but not limited to iPods, iPads, other tablets (e.g., Nook, Kindle, etc.), and MP3 players
- Optical storage media such as compact discs (CDs) and digital versatile discs (DVDs)
- Printers and copiers
- Fax machines
- Portable texting devices

5. Definition of District Electronic Device

The term "District electronic device" means any electronic device that is owned, leased, or rented by the District, purchased with funds from a grant approved by or awarded to the District, or borrowed by or loaned to the District from another agency.

6. Definition of District Electronic Network

The term "District electronic network" means the District's local area District-wide and Internet systems, whether hardwired or wireless, including software, email and voicemail systems, remote sites, and/or VPN connections.

OWNERSHIP

District EIR is District property provided to meet District needs. They do not belong to employees. Use of District EIR is a privilege which the District may revoke or restrict at any time without prior notice to the employee.

All District computers and District electronic devices are to be registered to the District and not to an employee. All software on District computers and District electronic devices is to be registered to the District and not to an employee, except as otherwise provided herein.

No employee shall remove a District computer or District electronic device from the District's property without the prior, express authorization of the employee's supervisor.

NO EMPLOYEE PRIVACY

Employees have no privacy whatsoever in their personal or work-related use of the EIR, or to any communications or other information contained in the District EIR or that may pass through District EIR. With or without cause and with or without notice to the employee, the District retains the right to remotely monitor, physically inspect, or examine District computers, electronic devices, network, or other EIR, and any communication or information stored on or passing through the District EIR, including but not limited to software, data and image files, Internet use, emails, text messages, and voicemail.

All email sent and received via the District email system, including email of a personal nature, will be captured and retained in a central location for a period of time determined by the District to be appropriate. Deletion of email from computers and electronic devices will not delete captured and retained email. The email that is captured and retained in a central location is the District's official record of such email, no matter where other copies of such email may be found.

District EIR will be inspected for software and/or virus-like programming, including commercial software applications ("Apps") that harvest, collect, or compromise data or information resources. Any computer or electronic device containing those elements

may be disconnected, blocked, or otherwise isolated at any time and without notice, in order to protect District EIR.

When an employee leaves employment with the District, management shall be given access to and the authority to dispose of any and all District electronic records, including the employee's computer files, email, voicemail, text messages, and any other electronic information stored on District computers and devices. Employees leaving their employment shall provide to District all files and other electronic records from personal computers and devices, and employees shall not delete such items from District EIR.

ONLINE/INTERNET SERVICES: USER OBLIGATIONS AND RESPONSIBILITIES

Employees are authorized to use district equipment to access the Internet or other online services in accordance with Board policy, the district's Acceptable Use Agreement, and the user obligations and responsibilities specified below.

1. The employee in whose name an online services account is issued is responsible for its proper use at all times. Employees shall keep account information, home addresses, and telephone numbers private. They shall use the system only under the account number to which they have been assigned.

2. Employees shall use the system safely, responsibly, and primarily for work-related purposes.

3. Employees shall not use the system to threaten, intimidate, harass, or ridicule students or other staff. Employees shall not access, post, submit, 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.

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

5. Employees shall not use the system to engage in commercial or other for-profit activities without permission of the Superintendent or designee.

6. Copyrighted material shall be downloaded and/or posted online only in accordance with applicable copyright laws.

7. Employees shall not attempt to interfere with other users' ability to send or receive

email, nor shall they attempt to read, delete, copy, modify, or forge other users' email.

8. 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.

9. Users shall report any security problem or misuse of the services to the Superintendent or designee.

PERSONAL USE

Employees shall use District EIR primarily for purposes related to their employment. District laptop computers and portable electronic devices shall be used solely by authorized employees and not by family members or other unauthorized persons.

Where approved by the employee's supervisor in advance, an employee may make minimal personal use of District EIR as long as that use does not violate this Policy, does not result in any additional fee or charge to the District, and does not interfere with the normal business practices of the District or the performance of the employee's duties. As described in this Policy, employees have no privacy whatsoever in their personal use of District computers, electronic devices, and network, including but not limited to software, data and image files, internet use, text messages, and emails. As noted herein, all emails sent and received via the District email system are captured and retained by the District.

PASSWORD PROTECTION

To protect against unauthorized use and/or access to District electronic records, all District computers and electronic devices capable of being password protected shall be password protected, even if a computer or electronic device is assigned to a single employee for his or her sole use. Any screen saver capable of being password protected shall be password protected in addition to any network log-in requirement. Whether or not password protection is technologically feasible, the employee to whom the

computer or electronic device is assigned shall be responsible for physically protecting it against unauthorized use and unauthorized access to District electronic records.

Since the District needs the ability to access its own equipment, each employee shall be responsible for registering their user password(s) with their immediate supervisor, whether the password protection is at the system or program level.

SOFTWARE AND ELECTRONIC DEVICES

Software, computers, and electronic devices must meet specific standards to protect the District's network and other EIR.

Computers, cellphones, tablets, and similar devices, are capable of downloading, storing, and using various software, including Apps from both District-approved and non-approved providers. Some Apps are known to collect data from devices onto which they are loaded and from other devices to which the device is connected. Such collection, and any dissemination of collected data, is a threat to the confidentiality of electronic records stored on District EIR and a breach of information security. For this reason, employees shall not download non-approved Apps onto District computers or devices.

The Superintendent/Designee is authorized to approve employee requests for installation of non-District software on a case-by-case basis, subject to the following limitations:

1. Software shall not be installed without advance authorization from the Superintendent/Designee. Software not related to the mission, vision, and goals of the District shall not be installed.

2. No software shall be installed without written proof of licensing, which shall be retained by the technology administrator. Multiple installations of the same license number will be assumed to violate copyright unless a multiple license provision can be demonstrated.

3. Approval shall by limited, as follows:

    - The District shall ensure that the intended use of the software is consistent with the District's Mission, Vision, and Goals, and with all applicable policies and procedures.

    - The District has the right to remove the software at any time and for any reason without prior notice to the employee.

- The District has no obligation to return the software to the employee.

- If the employee is assigned to a different computer or electronic device, the District has no obligation to install the software on that equipment.

Employees who have been authorized to download and install software shall adhere to copyrights, trademarks, licenses, and any contractual agreements applicable to the software, including provisions prohibiting the duplication of material without proper authorization and inclusion of copyright notices in any use of the material.

FILTERS AND OTHER INTERNET PROTECTION MEASURES

To ensure that use of the District's network is consistent with the District's mission, the District uses content and/or bandwidth software to prevent access to pornographic and other websites that are inconsistent with the mission and values of the District. No employee shall bypass or evade, or attempt to bypass or evade, the District's filter system.

OTHER UNACCEPTABLE USES

In addition to other provisions of this Policy, employees using District EIR shall be responsible for using them only in compliance with the following requirements, unless the Superintendent/Designee gives prior express permission.

1. An employee shall use only his or her assigned account or password to access District computers, electronic devices, and network. No employee shall permit the use of his or her assigned account or password, or use another person's assigned account or password, without the prior express written consent of the employee's supervisor and the designated technology administrator at the employee's worksite.

2. Employees are prohibited from using District EIR for knowingly transmitting, receiving, or storing any oral or written communication that is obscene, threatening, or disruptive, or that reasonably could be construed as discrimination, harassment, bullying, or disparagement of others based on actual or perceived characteristics of race, ethnicity, religion, color, national origin, nationality, ancestry, ethnic group identification, physical disability, mental disability, medical condition, marital status, sex, age, sexual orientation, gender,

gender identity, gender expression, genetic information (or association with a person or group with one or more of these actual or perceived characteristics). This prohibition applies to written and oral communication of any kind, including music and images.

3. Employees are prohibited from using District EIR for knowingly accessing, transmitting, receiving, or storing any image file that depicts actual or simulated torture, bondage, or physical abuse of any human being or other creature, or that is sexually explicit or pornographic. This prohibition does not apply to technology department employees engaged in authorized tracking or investigative activities regarding technology usage history of another employee.

   A. "Sexually explicit" means a visual depiction of actual or simulated human sex acts, or the unclothed human genitalia, pubic area, anus, buttocks, or female breast that lacks serious artistic, literary, scientific, or political value.

   B. This prohibition applies to visual depictions of any kind, including screensavers, drawings, cartoons, and animations.

4. Employees shall not knowingly store, transmit, or download copyrighted material on EIR without permission of the copyright holder. Employees shall download copyrighted material only in accordance with applicable copyright laws.

5. Employees are prohibited from knowingly using EIR to intentionally access information intended to be private or restricted; change data created or owned by another user or any other agency, company, or network; make unauthorized changes to the appearance or operational characteristics of the District's system; load, upload, download, or create a computer virus; alter the file of any other user or entity; or remove, change, or add a password, alter system settings, preloaded software settings, firmware, and hardware without prior approval of the designated technology administrator at the employee's worksite.

6. Employees are prohibited from remotely accessing the District electronic network without prior express approval of the Superintendent/Designee.

7. Employees are prohibited from uploading to a non-District server any file contained on a District computer or server, whether the file is work related or personal, without prior approval of the Superintendent/Designee. This

prohibition is not intended to prevent uploads or file copying for appropriate work-related purposes.

8. Any text transmission can only be used by an authorized District messaging system and/or device.

9. Employees also are prohibited from using EIR for the following:

- Personal financial gain
- Commercial advertising
- Political activity as defined in Education Code Sections 7050-7058
- Religious advocacy
- Promoting charitable organizations
- Communicating in someone else's name
- Attempting to breach network security
- Creating, sending, or receiving materials that are inconsistent with the mission and values of the District
- Mass distribution of email to a school site without prior approval of the site administrator
- Mass distribution of email to the District without approval of the Superintendent/ Designee
- Any activity prohibited by law, board policy, or administrative regulation, or the rules of conduct described in the Education Code

APPROPRIATE USE OF PERSONAL COMPUTERS AND DEVICES, PUBLIC RECORDS, AND COLLECTION OF DISTRICT ELECTRONIC RECORDS

This Policy also applies, to the extent described, hereinafter, to any employee personal computer or electronic device that either contains District electronic records or is being used with or connected to the District's EIR, and also applies to the use of personal computers and devices while they are physically located on District property.

Staff Use of Personal Devices

"Device" means a privately owned wireless and/or portable electronic piece of equipment that includes laptops, notebooks, tablets/slates, iPod Touches, cell phones, smart phones, and any other related technology.

Staff members bring personal devices to their work site at their own risk. The District is not responsible if an electronic device or other item that is lost, stolen or misplaced.

The District has a responsibility to protect its network and technical resources. Any

employee who utilizes his/her own personal device for any employment-related purpose at a District work site is required to adhere to the current Acceptable Use Policy (AUP) and Personal Device Policy (PDP) of the District. The District Technology Department will provide instructions on how to connect a personal device to the District network when a signed Acceptable Use Policy and a signed Personal Device Policy (PDP) have been returned.

When using a personal device, staff members must use the district wireless network. The device will be required to connect to the schools wireless network; the use of other wireless networks is not permitted. Personal devices will have access to the web-based software used by the District (web e-mail, web attendance, library search tools, etc.). Personal devices will not be able to access network files or printers.

Personal devices shall not be used to record, transmit or post photos or video of any employee or student at any time. Images or video recorded at a work site shall not be transmitted or posted at any time using a personal device without the express permission of the superintendent or designee.

While use of personal computers and other personal devices for District business is permitted, employees are advised that any and all District records contained on any device are the property of the District and their disclosure may be required. Employees have no expectation of privacy in such records. District business communications and records may constitute "Public Records" under the California Public Records Act, and may be records the District is required to maintain under applicable law, including Regulations under Title 5 of the California Code of Regulations. The District may be required to collect, disclose, produce and/or store such records, regardless of the ownership of the computer or device on which the records are located. There is no expectation of privacy in any public record located on a personal computer or device.

Use of an employee's personal email account to send or receive email related to District business could result in the personal email account containing records potentially deemed to be public records subject to collection and disclosure or District retention. Such email shall be forwarded to the District email system; unless the email already reflects it is sent from or is copied to the District email system. The forwarded or copied email becomes the official District record of such email, would be retained by the District email system, and such email on the employee's personal email system, and/or reflected in the personal computer or device, would only be only a duplicate copy, not subject to required collection in response to a public records request, and should

thereafter be deleted from the employee's personal email account. In such instances, there should be no expectation of privacy in the email.

If the employee works on, prepares, creates or possesses on a personal computer or device an electronic record in any form pertaining to District business, that record would potentially be deemed a public record or record subject to collection, disclosure or District retention. In such instances, there should be no expectation of privacy in the District electronic record, in any form or format, located on an employee's personal computer or device. The employee shall transmit such record in electronic format to the District upon request, which transmission may be through use of the District email system, or other means, and the employee shall thereafter delete the record from the employee's personal computer or device.

All personal computers and electronic devices that are connected to the District EIR, including the email system, or which otherwise contain District electronic records or access thereto, shall have user passwords installed and utilized to preclude unauthorized access to and/or use of the personal computer or device and/or its connection to District EIR. Whenever possible, individual programs, Apps, and/or connections on such computers and electronic devices shall each be password protected, requiring manual entry of a password before the computer or device can connect to any District EIR, including email, or access to any District electronic records. Whether or not password protection is technologically feasible, the employee who owns a computer or electronic device capable of connecting to EIR, or which contains District electronic records, shall be responsible for physically protecting it against unauthorized use.

Computers, cellphones, tablets and similar devices are capable of downloading, storing, and using various software, including Apps from both District-approved and non-approved providers. Some Apps are known to collect data from devices onto which they are loaded and from other devices to which the device is connected. Such collection, and any dissemination of collected data, is a threat to the confidentiality of District electronic records stored both on District EIR and on personal computers and devices used with and/or connected to District EIR, or which themselves contain District electronic records, and may constitute a breach of information security. For this reason, employees are discouraged from downloading non-approved Apps onto personal computers and devices that may contain District electronic records or be connected to or used with District EIR. Employees are responsible to ensure no District electronic records are compromised by the employee's use of personal computers or devices.

With the following exceptions, only the Superintendent/Designee may authorize installation or maintenance of either hardware or software on District or personal computers and electronic devices:

- Employees required by the District to have personal electronic devices may install such connection software as required to permit uploading, downloading, and syncing their required devices with a District computer;

- Employees required by the District to have personal electronic devices will be provided authorized software, including authorized Apps for the devices; downloading non-authorized Apps onto such devices is not permitted.

- Unauthorized connection of personal electronic devices to District EIR other than email, whether hardwired or wireless, is not permitted and employees who connect such devices, or install related software on District computers, are at risk of the computer being isolated from the District network and having connection and use rights limited, restricted, or removed; other potential disciplinary action may result if an employee takes such action without consent, or if the actions of the employee result in a breach of network security, release of confidential information, or violation of copyrights;

- Employees authorized to connect personal electronic devices to District EIR may be required to install appropriate security protection software on the device and the chief technology administrator may, in his/her discretion, elect to provide the required security protection software.

Certain activities may be permissible for use of personal computers or devices while physically located on or in District property or sites, as long as that use does not violate this Policy, does not result in any additional fee or charge to the District, and does not interfere with the normal business practices of the District or the performance of the employee's duties.

No employee shall, while physically located on or in a District facility use a personal computer or device or personal internet connection to do any of the following:

1. Knowingly transmitting, receiving, or storing any oral or written communication that is obscene, threatening, or disruptive, or that reasonably could be construed as discrimination, harassment, bullying, or disparagement of others based on actual or perceived characteristics of race, ethnicity, religion, color, national

origin, nationality, ancestry, ethnic group identification, physical disability, mental disability, medical condition, marital status, sex, age, sexual orientation, gender, gender identity, gender expression, genetic information (or association with a person or group with one or more of these actual or perceived characteristics). This prohibition applies to written and oral communication of any kind, including music and images.

2. Knowingly accessing, transmitting, receiving, or storing any image file that depicts actual or simulated torture, bondage, or physical abuse of any human being or other creature, or that is sexually explicit or pornographic.

   A. "Sexually explicit" means a visual depiction of actual or simulated human sex acts, or the unclothed human genitalia, pubic area, anus, buttocks, or female breast that lacks serious artistic, literary, scientific, or political value.

   B. This prohibition applies to visual depictions of any kind, including screensavers, drawings, cartoons, and animations.

3. Knowingly store, transmit, or download copyrighted material without permission of the copyright holder. Employees shall download copyrighted material only in accordance with applicable copyright laws.

4. Knowingly access information intended to be private or restricted; change data created or owned by another user or any other agency, company, or network; make unauthorized changes to the appearance or operational characteristics of the District's system; load, upload, download, or create a computer virus; alter the file of any other user or entity.

5. Accessing the District electronic network without prior express approval of the Superintendent/Designee.

6. Employees are prohibited from uploading to a non-District server any file contained on a District computer or server, whether the file is work related or personal, without prior approval of the Superintendent/Designee. This prohibition is not intended to prevent uploads or file copying for appropriate work-related purposes.

7. Engaging in any of the following activity:

   - Attempting to breach network security

- Mass distribution of email to a school site without prior approval of the site administrator
- Mass distribution of email to the District without approval of the Superintendent/ Designee
- Any activity prohibited by law, board policy, or administrative regulation, or the rules of conduct described in the Education Code.

DISCLAIMER

The District makes no guarantees about the quality of the EIR provided and is not responsible for any claims, losses, damages, costs, or other obligations arising from employee use of the resources. Any charges an employee accrues due to personal use of District EIR are to be borne by the employee. The District also denies any responsibility for the accuracy or quality of the information obtained through employee access.

VIOLATION OF THIS POLICY

Violations of this Policy shall be promptly reported to management personnel. Management personnel shall then promptly report violations of this Policy to the Superintendent/Designee.

Employees who violate this Policy are subject to discipline, up to and including termination, pursuant to the provisions of applicable laws governing employee discipline, and applicable District policies, procedures, and collective bargaining agreements. An employee's use of District EIR may also be restricted, suspended, or revoked.

DELANO JOINT UNION HIGH SCHOOL DISTRICT

Regulation approved: January 22, 2008
Delano, California

Revised regulation approved: May 14, 2013
Delano, California

Revised regulation approved: September 10, 2013
Delano, California