PERSONNEL

EMPLOYEE ACCEPTABLE USE POLICY FOR COMPUTERS, ELECTRONIC DEVICES, NETWORK, AND OTHER ELECTRONIC INFORMATION RESOURCES

The District recognizes that electronic information resources can enhance productivity, facilitate professional communication, and assist in providing quality educational programs, and are essential to many online or distance learning 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 devices under certain circumstances.

DEFINITIONS

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

2. The term "district electronic record" means any writing containing information relating to conduct of the District's business where the writing was prepared, owned, used, or retained in electronic/digital format by the District, regardless of where or how the record may have been prepared or where the record is retained. Records containing no more than incidental references to the District are not considered district electronic records. For this purpose, "writing" means anything in an electronic/digital format including sounds, images, symbols, words, or any combination thereof, specifically including electronic mail (email) and all other forms of electronic files. Recordings made of an employee's live interaction or other online presentations for distance learning purposes are district electronic records.

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

4. The term "district computer" means any computer 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 it is equipped with a modem or communication peripheral capable of digital connection.

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

- Telephones
- Cellphones, including “smartphones”
- Radios
- Pagers
- Digital cameras
- Personal digital assistants
- 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 or eReaders (e.g., Nook, Kindle, etc.), and MP3 players
- Optical storage media such as compact discs (CDs) and digital versatile discs (DVDs)
- Internet “hotspots” such as from Kajeet, AT&T, Verizon, and T-Mobile that allow a user to connect to the internet via a mobile device
- Printers and copiers
- Scanners
- Fax machines
- Portable texting devices

6. The term “district electronic device” means any electronic device 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.

7. The term “district electronic network” means the District’s local area district-wide network and internet systems, whether hardwired or wireless, including software, email and voicemail systems, remote sites, and/or “virtual private network” (VPN) connections, and without regard to the manner of connection.

8. The terms “personal computer” and “personal electronic device” mean computers and/or devices as defined in this policy that are not district computers or electronic devices, typically computers and/or devices owned by individuals including employees and visitors. Personal cell or smartphones, iPads, and similar devices are personal electronic devices, whether or not supported by a district stipend paid to the employee.

9. The term “VPN” means any combination of hardware and/or software that permits a computer or device to remotely connect to all or part of the district’s electronic network.

10. The term “distance learning” means any form of remote learning program where students may use or connect to District’s EIR while off campus, whether the remote program is a full or part-time synchronous virtual classroom, a version of independent study, asynchronous instruction, or any other technology-based remote learning program.

OWNERSHIP

District EIR is district property provided to meet district needs and does 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 in this policy.

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

NO EMPLOYEE PRIVACY

Employees have no privacy whatsoever in their personal or work-related use of district EIR, or to any communications or other information contained in 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 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 the email, no matter where other copies of that 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. This includes personal computers and/or electronic devices that an employee may connect, with or without proper authorization, to district EIR. Due to the commonplace presence of such software and Apps on personal computers and/or devices, their connection to district EIR without prior authorization is discouraged.

At no time, including when an employee leaves employment with the District, shall the employee delete district electronic records unless expressly authorized to take such action. 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 EIR. Employees leaving their employment shall provide the District with all files and other electronic records from personal computers and devices, and employees shall not delete those items unless expressly authorized to take such action. Video/audio recordings made by employees during delivery of online distance learning sessions are required to be kept for a minimal period, then to be deleted. Administration will determine these time frames and employees will comply with the time frames set by Administration.

PERSONAL USE

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

When 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. Should an employee use district EIR to access personal software, websites, Apps, social media, or other personal accounts, the employee shall be responsible for any disclosure of district electronic records, including student records, resulting from that use. As described in this policy, employees have no privacy whatsoever in their personal use of district EIR, including but not limited to software, data and image files, internet use, text messages, and emails. As noted in this policy, all emails sent and received via the district email system are captured and retained by the District.

PROPER CARE OF COMPUTERS AND DEVICES

All computers, devices, cases, chargers, and district-provided accessories must be returned on request. Employees who leave employment for any reason must return all district computers, devices, accessories, and district electronic records.

If an employee fails to return any district EIR on request, that employee may be subject to discipline and civil liability for damages arising from unauthorized information on or access through the district EIR including VPN connections. The employee may be required to pay the replacement cost of the EIR, or, if applicable, any insurance deductible. The employee may be held liable for fines, assessments, or damages collected from or assessed to the District arising from the loss or unauthorized disclosure of protected data and records.

General Precautions

In general, employees should:

- Only use a clean, soft cloth to clean the screen, no cleansers or liquids of any type.
- Cords and cables must be inserted carefully to prevent damage.
- EIR and cases must remain free of any writing, drawing, stickers, or labels that are not the property of the District.
- EIR should always be locked or supervised directly by the employee to whom it is assigned.
- District EIR should never be left in an unlocked locker, unlocked car, any unsupervised area, or anywhere where it is likely to be stolen or accessed without authorization.

Carrying Devices

- The protective cases provided with computers and devices have sufficient padding to protect the equipment from normal treatment and provide a suitable means for carrying the equipment. The guidelines below should be followed:

    - Computers and devices should always be in the protective case provided by the District when being transported or not being used.
    - No other items should be stored or carried in the case to avoid pressure and weight on the screen.

PASSWORD AND DEVICE PROTECTIONS

To protect against unauthorized use of and/or access to district EIR and electronic records, all district computers and electronic devices that can be password protected must be password protected, even if a computer or electronic device is assigned to a single employee for his or her sole use.

All personal computers and electronic devices connected to district EIR, including the email system, or which otherwise contain district electronic records or access to those records, 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 personal 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 to any district electronic records. District passwords should be different from personal passwords.

Any screensaver that can be password protected must be password protected in addition to any network login requirement. Whether or not password protection is technologically feasible, the employee who owns a computer or electronic device that can be connected to

district EIR, or that contains district electronic records, shall be responsible for physically protecting it against unauthorized use.

The Superintendent/designee may authorize and require installation of special software on district devices to enable remote shutdown to prevent unauthorized disclosure of district records should the device be lost or stolen. The Superintendent/designee may authorize installation of special software on personal devices that may contain district records, or have access to district records, to enable remote shutdown should the device be lost or stolen. Employees shall promptly report to their supervisor when district EIR or any personal computer or device containing district records or connections is lost or stolen.

SOFTWARE AND ELECTRONIC DEVICES

Software, computers, and electronic devices must meet specific standards to protect the District's electronic network and other EIR. In addition, violations of software copyright law have the potential of costing the District millions of dollars.

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. That 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. If an employee downloads a non-approved App onto a district computer or device, the employee may be held personally liable for any resulting unauthorized disclosure of district electronic records, including student records, in addition to any disciplinary actions taken for the unauthorized download.

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 that no district electronic records are compromised and no confidential information is inappropriately disclosed or breached because of the employee's use of personal computers or devices or any software downloaded onto them.

The Superintendent/designee is authorized to approve employee requests for installation of non-district software onto district computers and devices, subject to the following limitations:

1. Software not related to the mission of the District shall not be installed.

2. No software shall be installed without written proof of licensing, which shall be retained by the designated 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 be limited, as follows:

- 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 non-district 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/or 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. This prohibition includes the use of personal computers, devices, or internet connections to access inappropriate content while in a district facility.

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/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 only download copyrighted material 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; remove a password; or 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. For distance learning purposes, employees may be given permission to work remotely and use and access district EIR, subject to these acceptable use rules.

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 designated technology administrator at the employee's worksite. This prohibition is not intended to prevent uploads or file copying for appropriate work-related purposes. For example, during distance learning program delivery employees may record live sessions with students and other staff, and these recordings shall not be downloaded to a personal system or device and shall not be shared outside the district EIR.

8. Any text transmission concerning a district matter should be done using an authorized district messaging system and/or device, and must be done in a manner that protects the confidentiality and future recoverability of the message.

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

- Personal financial gain
- Commercial advertising
- Political activity as defined in California Education Code Sections 7050-7058
- Religious advocacy
- Promoting charitable organizations without prior authorization
- 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, administrative regulation, or the rules of conduct described in the Education Code, including the unauthorized sharing or disclosure of district electronic files.

10. Employees are prohibited from using personal computers, devices, or internet connections for any unacceptable use identified in this policy while physically located on or in a district facility.

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

To the extent described, this policy also applies to an employee's personal computer or electronic device that either contains district electronic records or is being used with or connected to district EIR, and also applies to the use of personal computers and devices while they are physically located on district property. Without limitation, this includes personal cellphones or other devices whether or not use of the device is supported by a district stipend.

While use of personal computers and other personal devices for district business is permitted, it is also discouraged. Employees are advised that any and all district electronic records contained on any personal device are the property of the District and their disclosure and recovery 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 which the District is required to maintain under applicable law, including Title 5 of the California Code of Regulations. The District may

be required to collect, disclose, produce, and/or store those 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. Upon request, employees will search personal computers, personal devices, and personal email and messaging systems for the presence of district electronic records and deliver them to the District.

For example, 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 and 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 the email, will 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 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, employees have no expectation of privacy in the email.

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

When an employee is requested to search for public records on a personal computer or device, a personal server, or in personal email or other accounts, the employee shall conduct a search for the records in a timely manner and may report on the search results in one or more of the following ways: 1) delivering the located public records to the District, or 2) providing an affidavit stating that no public records were found, or 3) providing an affidavit with sufficient information about a record to show it should not be deemed a public record.

Only the District's designated technology administrator is allowed to authorize installation or maintenance of either hardware or software on district or personal computers and electronic devices, with the following exceptions:

- Employees required by the District to have personal electronic devices may install such connection software 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 discouraged;

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

Certain activities on personal computers or devices while those devices are physically located on district property or sites may be permissible as long as those activities do not violate this policy, do not result in any additional fee or charge to the District, and do not interfere with the normal business practices of the District or performance of the employee's duties. For example only, while physically located on or in a district facility, employees may use a personal device to check personal email or take a call.

NOTICE REGARDING USE OF GOOGLE AND OTHER THIRD PARTY "CLOUD" PRODUCTS AND SERVICES

1. The District has elected to use a variety of outside vendors who provide websites, web-based software, and other services which may include mobile Apps, all of which are referred to as "cloud" services. The District is using various cloud products and services, including Google products and services, for both internal purposes and instructional use with students. As providers of those products or services, these vendors are acting as school officials under contract for the required services. Student records may properly be shared with school officials, including district employees and others who have a legitimate educational or other legally authorized purpose and who may need the records to perform the tasks for which they are employed or contracted.

Outside vendors who may have access to particular records have a formal written contract with the District to provide defined services or functions outsourced by the District, and may include consultants, insurance carriers, claims adjusters, accountants, attorneys, investigators, or others, including third party cloud vendors and service providers of online educational software and/or services that are part of the District's educational program, or who manage certain data stored in a secure cloud computing or web-based system for the District (e.g., Google is a third party vendor/school official).

Written contracts for third party cloud providers include significant privacy requirements intended to protect student information from unauthorized disclosure and use. While the District endeavors to protect student information, the use of internet connections and the presence of links in online products and services, the ease in accessing other websites and services without such protections, the potential presence of unapproved Apps on computers

and devices, and the ability of students and others with lawful access to inappropriately use or share student information outside the District's control will always be present.

The District intends that no student information will be inappropriately shared or used. For confidentiality purposes, student information includes both "personally identifiable information" and "covered information." Both personally identifiable and covered information are routinely disclosed to school officials in the course of initiating and using cloud services.

- "Personally identifiable information" includes but is not limited to a student's name, the name of the student's parent or other family members, the student's address, a personal identifier (such as the student's social security number), student number or biometric record, indirect identifiers (such as the student's date of birth, place of birth, and mother's maiden name), other information that alone or in combination is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or information requested by a person who the agency reasonably believes knows the identity of the student to whom the education record relates.

- "Covered information" includes personally identifiable information or material in any media or format that is created or provided by a student, or the student's parent or legal guardian, or is created or provided by an employee or agent of the District, or which is descriptive of a student or otherwise identifies a student, including educational records or email, first and last name, home address, telephone number, email address, or other information that allows physical or online contact, discipline records, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security number, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, or geolocation information.

2. Employees should make themselves aware of the presence or absence of student information in their use of Google and other cloud products and services. Any communication containing student information made with persons inside or outside the District, including via email or any Google App for sharing information, should be made only with persons legally entitled to receive the student information without violating rules against unauthorized disclosure. Student information shared by an employee with anyone outside the District without express permission from the designated technology administrator at the employee's worksite is shared at the employee's own risk. Sharing recorded distance learning live sessions on personal social media or otherwise outside the district EIR is strictly prohibited.

3. Employees will only log into district Google and other cloud products and services using their assigned district Google or other cloud login information, which will be different

from their regular district login information; employees will not log into district Google or other cloud products and/or services using any personal or non-assigned Google login information.

4. Employees will not log in to district Google and other cloud products and services using any personal computer or personal device that contains non-district Google or other cloud products or services without express permission from the designated technology administrator at the employee's worksite.

5. When using district Google products and services, employees may be exposed to links to other Google Apps that are not part of the G Suite core Apps or sites. Those linked Apps and sites are not required to be secure or confidential and may collect and share sensitive information, including student educational records, student covered information, or employee sensitive information. Employees will not use links or access non-G Suite Apps or sites and will immediately exit any linked Apps or sites if accessed.

6. Employees understand that their use of district EIR is subject to this policy and that its terms take precedence over anything to the contrary contained or represented in any Google or other cloud product documents or policies.

7. Employees understand that email and documents created within district Google products and services are not maintained in or on district EIR, that they are stored within the architecture of the Google products and services and that the District has no control over the safety, security, or maintenance of the email and documents. Email and documents pertaining to the business of the District, including student instructional material, may be public records that may be required to be retained; employees shall not delete or discard public or other records that require retention by the District.

8. Employees who are designated or otherwise become administrators of a Google network within the District shall make all privacy and other settings the most restrictive and protective of student information unless expressly authorized otherwise by an administrator at district cabinet level.

9. Employees working with a district Google or other cloud application shall not attempt to bypass or avoid the privacy settings of the App.

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 district EIR. 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

Violation of this policy shall be promptly reported to management personnel. Management personnel shall then promptly report any violation of this policy to the Superintendent/designee.

Employees who violate this policy are subject to discipline, up to and including termination of their employment pursuant to the provisions of applicable laws governing discipline and applicable district policies, procedures, and collective bargaining agreements. An employee's use of district EIR may also be restricted, suspended, or revoked, resulting in reassignment of the employee to a position not requiring use of EIR.