PARENT/GUARDIAN CONSENT AND STUDENT ACCEPTABLE USE POLICY AND AGREEMENT

INTRODUCTION

All statements and policies in this Consent and Student Acceptable Use Policy and Agreement govern Student use of district electronic information resources ("EIR") including the internet, whether Student is accessing the district EIR via district technology or via personal electronic devices, and whether Student is on or off campus at the time.

Students should expect no privacy whatsoever in their files, email, or in any use of the District's EIR. All student use of district EIR may be supervised and monitored; monitoring resources, including internet usage, can reveal all activities students engage in while using the District's EIR. Individuals or teams of teachers may set additional requirements for use in their classrooms.

PLEASE READ THIS DOCUMENT CAREFULLY

By signing the agreement accompanying this policy, parents and students agree to abide by and follow all rules and standards in this policy and consent to such use.

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

Use of the District's EIR, including the internet, is a privilege, not a right. If Student violates any term or condition in this policy, privileges may be terminated, access to district EIR may be denied, and Student will be subject to appropriate disciplinary action up to and including suspension and/or expulsion. When applicable, law enforcement agencies may become involved. If Student is enrolled in a remote learning program, such as distance learning or independent study using district EIR, and should Student lose EIR privileges, Student may be assigned to a classroom-based educational program within the District.

DEFINITIONS

The term "EIR" includes district computers, electronic devices, the software found on district computers and devices, and the District's electronic network.

The term “computer” means any computer, including a desktop, laptop, or Chromebook.

The term “district computer” means any computer owned, leased, or rented by the District.

The term “electronic device” means any device, other than a computer, capable of transmitting, receiving, or storing digital media. Electronic devices include but are not limited to telephones, cellphones, including “smartphones,” radios, pagers, digital cameras, personal digital assistants, portable storage devices, portable media devices, including but not limited to iPods, iPads, other tablets or eReaders 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, fax machines and scanners, and portable texting devices.

The term “district electronic network” means the District’s local area and wide area network and internet systems, whether hardwired or wireless, including software, email, and voicemail systems, remote sites, and/or “virtual private network” (VPN) connections.

The terms “personal computer” and “personal electronic device” mean computers and/or electronic devices as defined in this policy that are not district computers or electronic devices, typically computers and/or devices owned by individuals including students and visitors, and include without limitation personal cell or “smartphones,” iPads, etc.

The term “distance learning” means any form of remote learning program where students may use or connect to district 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.

In consideration for being provided with access to district EIR for use while a student of the District, Student and parents hereby agree as follows:

OWNERSHIP

District EIR is district property provided to meet district needs and does not belong to students. Use of district EIR is a privilege which the District may revoke or restrict at any time without prior notice to Student.

All district computers and district electronic devices are registered to the District and may be assigned to Student for classroom or distance learning use. All software on district computers and district electronic devices is registered to the District and not to Student, except as may be otherwise provided in this policy. Student shall not remove a district computer or district electronic device from district property without the prior express authorization of Student's teacher unless the computer and/or device has been assigned to Student for use during distance learning pursuant to a loan agreement.

NO STUDENT PRIVACY

Students have no privacy whatsoever in their personal or school-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 Student, the District retains the right to remotely monitor, physically inspect, or examine district computers, electronic devices, district electronic 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.

During distance learning, district staff may record live sessions between teachers and one or more students for educational purposes, and these recorded sessions may be made available to Student's class and others with appropriate login credentials for that class.

All student use of district EIR, including in chatrooms, messaging systems, on social media, or email sent or received via any district email system, including email of a personal nature, may be captured and retained for a period of time determined by the District to be appropriate. Deletion of student communications from assigned computers and electronic devices will not delete captured and retained student communications.

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.

The District may also block personal computers and/or electronic devices that Student may connect, with or without proper authorization, to district EIR. Due to the commonplace presence of data mining software and Apps on personal computers and/or devices, their connection to district EIR without prior authorization is discouraged. If connecting to district EIR from home or other remote location, Student must use the school-provided computer or device unless expressly authorized in advance by Student's teacher.

When Student leaves the District, school administration shall be given access to and the authority to dispose of, or retain as required by law, any and all student electronic records, including Student's computer files, email, voicemail, text messages, and any other electronic information stored in, on, or through district EIR. Students leaving the District are permitted to retain copies of student-generated data and shall provide the District with any educational records from personal computers and devices, and Student shall not delete those items from district EIR.

STUDENT-GENERATED CONTENT

Should Student desire to retain electronic copies of student-generated electronic content (e.g., papers, reports, or other materials created in electronic format), Student should make a request through the teacher who will facilitate obtaining the requested items. Student-generated content not retained by a student may be deleted/destroyed following Student's departure from the District, except items required under law to be retained by the District.

PERSONAL USE

Student shall use district EIR exclusively for purposes related to Student's education and as directed by a teacher. District laptop computers and portable electronic devices which the District allows to be removed from campus shall be used solely by authorized students and not by family members or other unauthorized persons, except in connection with completion of Student's educational assignments, if required.

Only when approved by Student's teacher in advance may Student make even minimal personal use of district EIR. Personal use of district EIR without prior authorization violates this policy, as does any use that results in any additional fee or charge to the District, interferes with the District's normal business practices or Student's educational program, or results in an unauthorized disclosure of another student's information. As described in this policy, Student has no privacy whatsoever in personal use of district EIR. Recording and/or disclosing distance learning live or recorded sessions is inappropriate without the express consent of Student's teacher. Unauthorized recording is a violation of Education Code Section 51512 and this policy.

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, notebooks, 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, including student records stored on district EIR, is a threat to the confidentiality of electronic records and a breach of information security. For this reason, Student shall not download or attempt to download non-approved Apps onto district computers or devices.

FILTERS AND OTHER INTERNET PROTECTION MEASURES

To ensure that use of the District's electronic network and the internet is consistent with the District's mission, the District uses content filtering software to prevent access to pornographic and other websites that are inconsistent with the mission and values of the District. Student shall not 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 or connected to district EIR.

OTHER UNACCEPTABLE USES

Student is responsible for using the District EIR's only in compliance with the following requirements, unless Student's teacher gives prior express permission:

1. Student shall use only his or her assigned account or password to access district computers, electronic devices, and the District's electronic network. Student shall not share or permit the use of an assigned account or password, or use another person's assigned account or password, without prior authorization of Student's teacher. Student shall not access a personal account (e.g., social media, email, text, or other messaging systems) using district EIR.

2. Student is prohibited from using district EIR for knowingly transmitting, receiving, or storing any oral or written communication or depiction 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 material of any kind, including written, oral, or music and/or images.

3. Student is 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.

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

5. Student is prohibited from knowingly using district 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 Student's teacher.

6. A student creating a security breach or unauthorized disclosure of protected student information, whether using a personal computer or device or district EIR, will be subject to disciplinary action.

7. Student is prohibited from remotely accessing the District's electronic network without prior express approval. Students provided devices such as laptops and/or internet hotspots for use in distance learning are authorized to use the devices to connect to the District's electronic network for distance learning purposes.

8. Student is also prohibited from using district EIR for the following:

- Personal financial gain
- Commercial advertising
- Political activity as defined in 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.

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

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 student records or information to perform the tasks for which they are employed or contracted.

Outside vendors with 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 makes no guarantee that student information will not be inappropriately shared or used. For confidentiality purposes, student information includes

both “personally identifiable information” and “covered information” as those terms are defined herein. Both personally identifiable and covered information are routinely and appropriately disclosed to school officials.

- “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, student number, 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 a student 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.

Student should be aware of the presence or absence of student information when using third-party products and services. Any communication containing student information made with persons inside or outside the District, including via email or via any third-party App for sharing information, should be made only with persons legally entitled to receive the student information without violating rules against unauthorized disclosure. Student’s own information shared by Student with anyone outside the District without express permission from Student’s teacher is shared at Student’s own risk. In connection with use of district-provided cloud services:

1. Student will only log into district third-party products and services using Student’s assigned district third-party login information, which will be different from Student’s regular district login information, and will not log into district third-party products and/or services using any personal or non-assigned login information.

2. When using district third-party products and services, Student may be exposed to links to other third-party Apps that are not part of the contracted Apps or sites. Those Apps and sites are not under contract, not required to be secure or confidential, and may collect and share sensitive information including student educational records, student covered information, or student personally identifiable information. Student will not use those links or access non-approved third-party Apps or sites and will immediately exit any linked Apps or sites if accessed.

3. Student understands that 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 third-party documents or policies.

4. Student understands that email and documents created within district third-party products and services are not maintained in or on district EIR and are stored within the architecture of the third-party products and services, and that the District has no control over the safety, security, or maintenance of the email and documents. If Student desires to correct information or obtain copies of student-generated content, Student should first make a request through a teacher.

5. Email and documents pertaining to the business of the District, including student instructional material, may be public records and may be required to be retained by the District. Student shall not delete or discard public or other records that require retention by the District.

6. Students working with a district third-party App shall not attempt to bypass or avoid the privacy settings of the third-party App.

7. Student shall not share student information of other students outside the District or third-party network system without express authorization of Student's teacher.

In signing this Agreement, parents/guardians are expressly acknowledging the risks of cloud and other technology use and giving their consent to Student's use of district EIR, knowing some student information may be disclosed.

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 Student's use of the resources. Any charge Student accrues due to personal use of district EIR is to be borne by Student. The District also denies any responsibility for the accuracy or quality of the information obtained through student access.

VIOLATION OF THIS POLICY

Violation of this policy shall be promptly reported to a teacher who will then promptly report the violation to the Superintendent/designee.

Students who violate this policy are subject to discipline, including suspension or expulsion, pursuant to applicable laws and district policies governing student discipline. Student's use of district EIR may also be restricted, suspended, or revoked. While the District is doing distance learning, the loss of privileges could result in Student being assigned a technology-free program, including paper packets of work, or to classroom-based instruction.

WILLFUL DAMAGE

Students/parents are responsible for full payment for damages to or loss of district technology resources, including internet connections.