PARENT/GUARDIAN CONSENT AND STUDENT ACCEPTABLE USE POLICY AND AGREEMENT Updated July 2026

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

The District recognizes that electronic information resources ("EIR") can enhance productivity, facilitate student/teacher communication, and otherwise assist in providing quality educational programs. Use of the District's EIR, including the internet, is a privilege, not a right. The privilege of using EIR provided by the District is not transferable or extendible by Student to people or groups outside the District and all privileges terminate when Student is no longer enrolled in the District. This policy is provided to make all users aware of the responsibilities associated with efficient, ethical, and lawful use of district EIR.

BOARD APPROVED
7/21/26

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, andshould 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 notebook, whether or not it is equipped with a modem or communication peripheral capable of digital connection.

The term "district computer" means any computer owned, leased, or rented by the District, whether purchased with general district revenue or funds from a grant approved by or awarded to the District, or a computer borrowed by or donated to the District from another agency, company, or entity.

The term "electronic device" means any device, other than a computer, capable of transmitting, receiving, or storing digital media, whether or not it 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 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 cellular service provider such as AT&T, Verizon, and T-Mobile, Baicells LTE routers and antennas, 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 device" means any electronic device owned, leased, or rented by the District, whether purchased with general district revenue or funds from a grant approved by or awarded to the District, or a device borrowed by or donated to the District from another agency, company, or entity.

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.

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.

PASSWORD AND DEVICE PROTECTIONS

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

All personal computers or personal devices containing any student records, or that can be connected to the district electronic network including district email, must be password protected if they can be password protected. Any screensaver that can be password protected must be password protected in addition to any network login requirement.

Student's school passwords should be different from personal passwords. Whether or not password protection is technologically feasible, the student to whom the computer or electronic device is assigned shall be responsible for physically protecting it against unauthorized use and access to district EIR.

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 districtapproved 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.

The Superintendent/designee is authorized to approve student requests for installation of non-district software, subject to the following limitations:

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

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

Students 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 electronic network and the internet 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. 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 prohibited from uploading to a non-district server any file contained in district EIR, whether the file is school related or personal, without prior approval of Student's teacher. This prohibition is not intended to prevent uploads or file copying for appropriate school-related purposes.

9. 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.

APPROPRIATE USE OF PERSONAL COMPUTERS AND DEVICES

This policy also applies to Student's personal computer or electronic device being used with or connected to the District's EIR, and to the use of personal computers and devices while physically located on district property.

While use of personal computers and other personal devices for student educational purposes is permitted, it is also discouraged to maximize the safety and security of student records. For example, use of a student's personal email account or social media to send or receive communications or documents related to the District's educational program could result in the personal email or social media account containing records potentially deemed to be confidential student information, the unauthorized disclosure of which violates the law.

Any student authorized to use a personal computer or electronic device on campus, or who is issued a computer or device for remote distance learning purposes, is authorized to connect the computer or device to district EIR and shall be responsible for physically protecting it against unauthorized use, damage, or loss.

Because personal computers and devices are capable of downloading, storing, and using various software, including Apps from both district approved and non-approved providers, and because personal computers and devices commonly contain Apps known to collect data from devices onto which they are loaded, and from other devices to which the device is connected, use of personal computers and devices in connection with Student's educational program or while connected to district EIR is discouraged as that use may be a threat to the confidentiality of student electronic records stored both on district EIR and on the personal computers and devices used with and/or connected to district EIR. This may constitute a breach of information security. For this reason, students are discouraged from downloading non-approved Apps onto personal computers and devicesthat may be used in connection with district EIR. Student is responsible to ensure that nostudent electronic records are compromised and that no confidential information is inappropriately disclosed or breached by Student's use of personal computers or devices.

Superintendent/designee may authorize Student's 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 and does not result in any additional fee or charge to the District.

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 (such as the student's social security number), studentnumber 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 reasonableperson 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 theidentity 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. Student will not log into district third-party products and services using anypersonal computer or personal device that contains non-district third-party products or services without express permission from the designated technology administrator at Student's school.

3. 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.

4. 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.

5. 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.

6. 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.

7. Students who are designated as or otherwise become administrators of a third-party network within the District, or who are permitted to set privacy levels on their district account, shall make all privacy and other settings the most restrictive andprotective of student information unless expressly authorized not to do so by Student's teacher.

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

9. 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.

STUDENT USE OF ARTIFICIAL INTELLIGENCE (AI)

Permitted Use of AI Tools

Students may use AI tools only under the direct supervision of a teacher or authorized school staff member. Permitted uses include, but are not limited to:

- Generating ideas and brainstorming: Using AI to help spark ideas for stories, projects, or presentations.
- Drafting and revising written work: With teacher guidance, using AI to help with grammar, spelling, and sentence structure, but not to generate entire assignments. All final work must reflect the student's own understanding and effort.
- Summarizing information: Using AI to help understand complex texts or topics, provided the student can articulate the summarized information in their own words.

- Creating visual aids or presentations: Utilizing AI features to assist in designing graphics, slides, or other multimedia elements for school projects.
- Interactive learning activities: Engaging with AI-powered educational games or platforms designed to reinforce concepts.

Prohibited Use of AI Tools

The following uses of AI tools are strictly prohibited and will be considered a violation of this policy:

- Plagiarism: Using AI to generate entire assignments (e.g., essays, reports, creative writing) and submitting them as one's own original work.
- Cheating: Using AI to answer questions during tests, quizzes, or other assessments
- Generating inappropriate content: Using AI to create, access, or share content that is discriminatory, offensive, harmful, or violates school rules.
- Sharing personal information: Inputting or sharing any personally identifiable information (e.g., full name, address, phone number) with AI tools unless explicitly instructed and supervised by a teacher.
- Attempting to bypass or disable any school-provided safety filters or monitoring systems related to AI use.
- Unauthorized access: Using AI tools to attempt to gain unauthorized access to school networks, systems, or other students' accounts.
- Misrepresenting AI-generated content: Presenting AI-generated content as their own work without acknowledging the use of AI

When using AI tools, students are expected to:

- Always inform their teacher if they are using an AI tool for a school assignment or activity.
- Understand that AI tools are aids, and their own critical thinking and effort are essential.
- Review and verify all information and content generated by AI for accuracy and appropriateness.
- Report any inappropriate or concerning AI-generated content to a teacher immediately.
- Adhere to all school rules and policies, including those related to internet safety and academic integrity.

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 toclassroom based instruction.

WILLFUL DAMAGE

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

Students are not to modify, alter, or decorate District DIR. This includes, but not limited to, placement of stickers on devices or removal of District asset tags and/or labels.

AGREEMENT AND CONSENT

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

As a student, I have read, understand my responsibilities, and agree to follow all rules outlined in the Acceptable Use Policy.

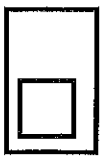
Student Name (Please Print):_____

Student Signature: _____

Date: _____

As a parent/guardian, I have read, understand the risks of, and give my express consent for participation of the undersigned student in the District's technology enhanced classrooms, including use of the internet and third-party participation via data storage and/or Student's use of online education products and services.

As a parent/guardian, I understand that I may "opt out" of allowing my student to take district EIR home by checking the box below. **I also understand that my student(s) will continue to use district EIR while at school and that I and my student(s) will remain responsible for the district EIR used at school.**



By checking this box I choose to "opt out" and understand that my child will not be able to use district EIR at home or in distance learning but will still be responsible for meeting all course requirements

Parent Name (Please Print):_____

Parent Signature:_____

Date: _____