IJNDB-R

REGULATION

USE OF TECHNOLOGY RESOURCES IN INSTRUCTION

(Safety and Use of Electronic Information Services)

Acceptable use of technology resources means technology must be used in a responsible, efficient, ethical, and legal manner and in accordance with the policies and educational goals of the District. This regulation is designed to guide qualifying students, employees and other users who acquire access privilege through association with the District in the acceptable use of the District's electronic information services (EIS), including computer systems, networks, and other technology resources. **This regulation also sets forth the acceptable uses of personal wireless communication devices, whether or not such devices access the District's EIS.**

Filtering, monitoring and access controls shall be established to:

- ~~Limit~~ **Restrict** access by minors to inappropriate/**harmful** matter on the Internet~~ and World Wide Web.~~
- Monitor the safety and security of minors when using electronic mail~~,~~ ~~chat rooms,~~ and other forms of direct electronic communications (e.g., wikis, blogs, on-line collaborative learning sites).
- Monitor for unauthorized access, including ~~so-called~~ "hacking," and other unlawful activities by minors online.
- ~~Restrict access by minors to materials harmful to minors.~~
- **Restrict student access to social media platforms except as allowed by the student's teacher to the extent necessary for educational purposes.**

Content Filtering

A content filtering program or similar technology shall be used on the District's networked EIS as well as on standalone computers capable of District authorized access to the Internet. The technology shall at a minimum limit access to obscene, profane, sexually oriented, harmful, or illegal materials. Should a District adult employee have a legitimate need to obtain information from an access-limited site, the Superintendent may authorize, on a limited basis, access for the necessary purpose specified by the employee's request to be granted access.

Installation of Software

Users may not install personal software onto District computers without first receiving the express permission of their administrator **and the Director of Educational Technology**. Users requesting permission to install personal software must provide the administrator with a copy of the software license that permits them to install the software. Files obtained from sources outside the District, including electronic storage devices brought from home and files downloaded from newsgroups or bulletin boards, may contain dangerous computer viruses and should never be downloaded onto District computers without prior approval. This is not intended to restrict the downloading of files from Internet sources or online services for use as curriculum supplements by teachers.

Duty Not to Waste District Resources

Users must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to sending mass mailings, printing multiple copies of documents, downloading lengthy files such as non-educational games, movies and music, streaming music or movies, or otherwise creating unnecessary network traffic.

Education, Supervision, and Monitoring

It is the responsibility of all District employees to be knowledgeable of the Board's policy and administrative regulations and procedures related to the use of technology resources. Employees are further responsible, to the extent prudent to an individual's assignment, to educate, supervise, and monitor student use of the District's online computer network. District, department, and school administrators shall provide employees with appropriate in-servicing and assist employees with the implementation of this Policy IJNDB and this regulation.

As a means of providing safety and security in direct electronic communications and to prevent abuses to the appropriate use of electronic equipment, all computer access to the Internet through the District's EIS or standalone connection shall be monitored periodically or randomly through in-use monitoring or review of usage logs.

Access Control

Individual access to the District's EIS shall be by authorization only. Designated personnel may provide authorization to students and staff who have completed and returned an annual Acceptable Use Agreement. The Superintendent may give authorization to other persons to use the District's EIS.

Employees leaving the District shall discontinue use of District technology upon

termination of employment. Access to the District's EIS will be removed.

Directory Information

The District designates the following personally identifiable information contained in a student's education records as "directory information" and may disclose that information without prior written consent [20 U.S.C. 1232g(a)(5)(A)]:

- The student's name.
- The student's address.
- The student's telephone listing.
- The student's date and place of birth.
- The student's electronic mail address.
- The student's photograph/image.
- The student's grade level.
- The student's major field of study.
- The student's dates of attendance.
- The student's enrollment status (e.g., part time or full time).
- The student's participation in officially recognized activities and sports.
- The student's weight and height if a member of an athletic team.
- The student's honors and awards received.
- The student's most recently attended educational agency or institution.

~~Absent unusual circumstances, a~~ **A** request to not disclose directory information from a student's educational records without prior written consent must be made in writing to the school principal by August 31st of each school year or for new students, within three weeks of enrollment. ~~If the parent(s)/legal guardian(s) have not indicated, in writing, refusal to allow the release of directory information, the District will assume it has permission to release the above-mentioned information.~~ This designation will remain in effect until it is modified by the signed and dated written direction of the ~~parent(s)/legal guardian(s)~~ **parent/legal guardian.**

Web Publishing

The District recognizes the value and potential of publishing on the Internet. School faculty and staff may create electronic home pages or group pages that seek to carry out official business and communication of the District's mission. All such pages must be accessible to the District, ~~parent(s/legal guardian(s)~~ **the parent/legal guardian**, and students from an official school website within the District. All staff publishers must adhere to the policies of the District, and must comply with all relevant federal and state laws. Web pages shall not display personally identifiable student information unless explicit and verifiable written permission has been granted by the student's ~~legal~~ parent/**legal** guardian. Web pages must reflect positively upon the District and school. E-mail addresses/links on web pages must be a cfsdl6.org address. The District provides computer services and networking to enhance the District's educational and administrative processes, and to improve communication with the world community. Material that fails to meet established educational objectives or that is in violation of a provision of District policy and administrative regulations will be removed.

Student Google Accounts

The District has created Google accounts for all students, with an alias to allow for collaborative sharing between students and their teachers. These accounts will be used at school for school-related projects, but may also be used by students outside of school with ~~parent(s)/legal guardian(s)~~ **the parent's/legal guardian's** permission.

The Google naming convention will be an alias with ~~first initial, last initial,~~ **a** series of numbers from student identification (ID) and a Catalina Foothills School District (CFSD) site domain. District-provided e-mail using the Google account can only be sent and received between students and teachers within CFSD. The password for each student's account will be shared with ~~parent(s)/**legal** guardian(s)~~ **the parent/legal guardian** to keep them informed about student use of this technological tool. This account will be considered the student's official CFSD Google account until such time as the student is no longer enrolled in Catalina Foothills School District.

See section on acceptable use in this regulation for acceptable and prohibited conduct. Access to and use of the student Google account is considered a privilege accorded at the discretion of the District. The District maintains the right to immediately withdraw the access and use of student Google account when there is reason to believe that violations of law or District policies have occurred. In such cases, the alleged violation will be referred to the principal for further investigation and adjudication.

Bring Your Own Device (BYOD)

The District's goal is to increase students' access to digital tools and facilitate more immediate access to technology-based information. To this end, the

District recognizes the value of allowing students and staff to bring their own devices to school to connect to the District's EIS. These devices are commonly referred to as Bring Your Own Device (BYOD) or personal electronic devices (PDs). The purpose of this section of IJNDB-R is to authorize and establish reasonable rules for students and staff to possess and use their PDs at school.

A PD is any electronic device owned by a student or his/her family or a staff member that stores, transmits, receives or displays voice messages, data, or images, or provides a wireless unfiltered connection to the Internet. This definition includes, but is not limited to, cellular telephones, digital audio players, digital cameras, laptop computers, tablet computers, pagers, portable game players, **smartwatches,** and any new technology developed with similar capabilities.

This regulation applies to a student's or staff member's use of a PD while 1) on school property (including buses), 2) at a school event, or 3) while using the District's network (including at home).

- A student or staff member is permitted to use a PD only after the student and a ~~parent(s)/legal guardian(s)~~ **parent/legal guardian** or staff member have signed and returned the annual Acceptable Use Agreement.
- In a classroom setting, a student ~~or staff member~~ may only use a PD for educational purposes at the direction of a teacher or administrator **or during an emergency.** Other than in a classroom setting on school property, the administration at each school ~~will determine~~ **will set limits on the use of a PD at school, including determining** where and when and for what purpose a student or staff member may use a PD. A school administrator or staff member always has the right to prohibit **a** student~~(s)~~ from using a PD at certain times or during designated activities that occur during the school day (e.g., school presentations/assemblies, theatrical performances, ~~or~~ guest speakers).
    - **In grades K-8, student PDs will remain "off and away" for the day.**
    - **In grades 9-12, student PDs will remain "off and away" from bell-to-bell during each class period of the school day. Students may access their PDs during lunch, passing periods, and before/after school.**
- In a classroom setting, a student or staff member is prohibited from using a PD to access the Internet using any external Internet service**, including cellular service**. In a classroom setting, a student using a PD, including a smartphone, may only access the Internet using the Wi-Fi access provided by the District.
- The student/owner of a PD is the only person allowed to use the device. Students are prohibited from sharing their assigned user name and/or password with others. A student must sign in to the designated PD District wireless network using his or her assigned username and password.
- If a student's use of a PD causes disruption in any setting, the student can be directed either to put the PD away and/or the PD can be

confiscated and the student referred to an administrator for further discipline.

- On school property, a student or staff member may not use a PD to connect to the District's network by a network cable plugged into a data outlet. Also, on school property, a student may not print from a PD.
- The District is not liable for any PD that is lost, loaned, damaged, or stolen. Each student or staff member is responsible for his or her own PD, including set-up, maintenance, charging, and security. Students will not be able to charge personal devices at school. Staff members will not store a student's PD, nor will any District staff diagnose, repair, or work on any PD. If a PD breaks while being used in school, the student or staff member will put the device away and take it home at the end of the school day where the student and the ~~parent(s)/legal guardian(s)~~ **parent/legal guardian** or staff member can troubleshoot the issue.
- The District is not responsible for the payment of any user fees or data charges associated with the use of a PD that are billed by a third party to a student and/or a student's ~~parent(s)/legal guardian(s~~) **parent/legal guardian** or staff member, even if the fees or charges were incurred by the student or staff member for an educational purpose.
- A student or staff member who violates a law, District policy, procedure, or school rule while using a PD will be disciplined pursuant to District policies. In addition, an administrator can revoke a student's PD privileges.
- Students or staff do not have any expectation of privacy in anything they create, store, send, receive, or display on or over the District's EIS.
- School officials may search and/or seize a student's PD if there are reasonable grounds for suspecting that the search or seizure will reveal evidence that the student has violated or is violating the law or a District policy, procedure, or school rule.

PDs are a supplement to the equipment already in use in the classroom. BYOD is an optional program for students and staff and ~~parent(s)/legal guardian(s)~~ **the parent/legal guardian** ~~are~~ **is** not required to purchase a device for their child. Students who do not have access to a PD will be provided with ~~comparable~~ District-owned equipment for classroom lessons that require access to technological resources. Access to or use of PDs will not be used as a factor in grading or assessing student work.

Social Media

Catalina Foothills School District (CFSD) recognizes that access to new learning technologies gives students and teachers greater opportunities to learn, engage, communicate, and develop skills needed for work, life, and citizenship. The District is committed to developing 21st Century technology and communication skills, including the use of "social media."

Use of social media requires a high level of responsibility and accountability. With this in mind, the District has developed the following guidelines to provide direction to employees and students when participating in web-based social medial activities.

Social media is the use of web-based and/or mobile technologies to communicate through interactive dialogue. Social media technologies include, but are not limited to, blogs, picture-sharing, vlogs, wall-postings, e-mail, instant messaging, music-sharing, crowdsourcing, voice over IP (VoIP), Facebook, LinkedIn, X, YouTube, Instagram, TikTok, and any successor protocol to transmit information. These technologies include any services or applications that: transmit sounds, images, texts, messages, videos, or electronic information; electronically records, plays, or stores information; or accesses the Internet or private communication or information networks used on any device, including smartphones, **smartwatches,** and tablets and other such mobile technologies and subsequent generations of these and related devices.

In this regulation, the term "*school-related social media*" means use of a District-approved social media site through the District's EIS. The term "*personal social media*" means all other use of social media, including an individual's own private and or commercial use of social media, not connected to the District's EIS. The term "*communication*" includes words, pictures, drawings, photographs/images, and videos.

Use of Personal Social Media
by District Employees:

- District employees are required to maintain a professional relationship with students. To maintain this professional relationship, an employee shall not "friend" or accept personal Facebook, X or other third-party social media requests from students. Employees shall redirect students to school-related social media sites approved by the District.

- The only exception to the rule above is that an employee may use personal social media to communicate with a student who is a relative or a close family friend, provided that 1) the ~~parent(s)/legal guardian(s)~~ **parent/legal guardian** of the student has indicated in writing that he or she is aware that an employee is communicating by personal social media with the student; 2) the content on the employee's personal social media site is appropriate; and 3) the employee informs the school site administrator that he or she is communicating with the student by means of personal social media. (For example, if the conditions of this paragraph are satisfied, it may be appropriate for a teacher who is also a student's aunt to "friend" the student on the teacher's personal Facebook page.)

- An employee shall not communicate in a manner that is unprofessional and would 1) disclose confidential or private information; 2) cause harm to students, ~~parent(s)/legal guardian(s)~~ **the parent/legal guardian**, employees, or other members of the school community; 3) significantly and adversely impact the employee's work-related reputation or the reputation of the District; 4) should not reflect ~~negitively~~ **negatively** on the employee, a colleague, student, or the District. These restrictions shall not be interpreted to prohibit any communication on a matter of public

concern when the employee's interest in engaging in the communication outweighs the District's interest in managing its work force effectively.

● Employees shall not expect personal social media communications that have been marked as "private" to remain private. It is not uncommon to have information in a personal "private" social media site to be disclosed to the District by a person within the personal "private" group, and the District may investigate the information further.

Use of School-Related Social Media by District Employees:

● Communications with other employees, individual students, ~~parent(s)/legal guardian(s)~~ **the parent/legal guardian**, and other members of the school community must always be professional in content and tone.

● An employee shall intervene to stop disrespectful, defamatory, discriminating, harassing, intimidating, bullying, vulgar and/or obscene behavior.

● Confidential or private information about students, employees, ~~parent(s)/legal guardian(s)~~ **the parent/legal guardian**, or other members of the school community shall not be disclosed by employees.

● Only social media sites approved by the District shall be used by employees. Sites are approved based on their educational content. All social media communications using the District's EIS may be monitored by the District.

● Communications with students shall be academic in nature and relate to school topics. *Employees shall avoid discussion of personal topics with students*.

● Employees shall ensure that their profile and related social media site are professional and consistent with how they wish to present themselves to other employees, ~~parent(s)/legal guardian(s)~~ **the parent/legal guardian**, and students and should not reflect negatively on the employee or the District. An employee's profile shall also be consistent with the mission of the District.

● Communications (e.g., blogs and wiki posts) shall be well written using Standard English**, Mandarin Chinese, and/or Spanish for school-related World Languages blogs, wikis, etc.** Writing conventions shall be followed, including proper grammar, capitalization, and punctuation.

● An employee shall use his or her real name and always be identifiable as an employee of the District.

● An employee shall acknowledge his or her mistakes, correct errors quickly, confirm receipt of updated or revised posts, and respond promptly to concerns about misinformation.

● The District's proprietary content and information (e.g., District assessments, curriculum, etc.) shall not be shared. Employees shall comply with copyright laws when using the creative works of others.

● Employees shall limit exposure of advertising to students and families.

● Employees shall follow the law, Board policies, and District regulations. Read and follow the "Terms of Service" of providers and, for teachers, ensure that students do the same.

● Employees shall stay informed and cautious about the emergence of new problems in the use of social media.

● Questionable conduct, contact, or content shall be reported by employees to a school site administrator.

Use of Social Media by Students:

Students are responsible for using good judgment and behavior when using social media and will be held accountable for statements and postings.

● *For school-related social media*. A student's school-related social media communication can be considered inappropriate if it violates existing behavior standards in the District's Student Handbook regardless of whether the communication occurs on or off school property. If a student's communication would be considered inappropriate inside the classroom or at school, then it is also inappropriate on a school-related social media site.

● *For personal social media*. **Students may use PDs to access social media platforms during the instructional time over the District's EIS only when allowed to do so by the student's teacher to the extent necessary for educational purposes.** A student's personal social media communication can be considered inappropriate**, regardless of when or where a social media post is made,** if it is reasonably likely to have, or does have a negative impact on the school environment and the communication:

■ promotes illegal drugs, illegal activities, violence, or drinking;

■ promotes or incites violence or causes personal harm or bodily injury;

■ involves prohibited discrimination, defamation, harassment, intimidation, threats or stalking;

- is obscene or vulgar; or

- disrupts a classroom, the school, or a District activity.

● A student should state/post only what he or she wants the world to see. ~~Parent(s)/legal guardian(s)~~ **The parent/legal guardian**, teachers, and administrators may visit a student's social media sites. Once something is shared, it should be assumed that it will be available for everyone to see, even if the information is only shared on a personal "private" site. Even after something is removed from a social media site, it may already have been copied or printed by others and may remain on the Internet permanently.

● When using school-related social media:

- Use social media for school-related purposes only. Avoid discussion of personal topics.

- Express opinions respectfully and treat others with dignity and respect.

- Use Standard English. Blog and wiki posts, for example, should be well written. Follow writing conventions, including proper grammar, capitalization, and punctuation.

- Be open and honest. Use a real name (and CFSD alias) and do not use someone else's identity.

- Accept responsibility. Acknowledge mistakes and correct errors quickly. Confirm receipt of undated or revised posts, and respond promptly to concerns and misinformation.

- Comply with copyright laws when using the creative works of others.

- Follow the "Terms of Use" of any third-party social media provider.

- Report questionable conduct, contact, or content to a teacher, administrator and/or ~~parent(s)/legal guardian(s)~~ **the parent/legal guardian**.

Search and Seizure

Searches and/or Seizures that Require Reasonable Suspicion

School officials may search and/or seize student property if there are reasonable grounds for suspecting that the search or seizure will reveal evidence that the student has violated or is violating the law or a District policy,

procedure or school rule. This authority extends to student-owned electronic/technology devices and electronic storage.

Searches and/or Seizures that Do Not Require Reasonable Suspicion

Students have no reasonable expectation of privacy concerning the following and may be inspected and/or searched at any time with or without notice, by school personnel:

- Electronic devices provided to students by the District, including computers, laptops and tablets, electronic storage devices (e.g., thumb drives, separate hard drives, etc.) and other electronic/technology devices.
- Communications (includes words, pictures, drawings, photographs/images, videos recordings, and sound files) that are sent, received, or created using the District's EIS, including District-created e-mail accounts, social media communications using the District's EIS, or District-created storage for electronic communications.

Acceptable Use

The use of the District's EIS is a privilege and not a right. The following sets out rules for District employees and students to follow to appropriately use the District's EIS. Each user of the District's EIS, including a user of a PD shall:

● Use the District's EIS to support personal educational objectives consistent with the educational goals and objectives of the District. **District internet and property may only be used for authorized activities; they may not be used for personal gain.**

● Abide by all copyright and trademark laws and regulations.

● Understand that electronic mail or direct electronic communication is not private and may be read and monitored by the District.

● Use electronic mail only for communications that are relevant and of interest to mail recipients.

● Follow District's policies, school rules, and behavior standards set out in the District's student handbooks.

● Observe all applicable state or federal laws.

● Obtain permission to record, transmit, or post photos or a video of a person with any electronic device.

● Obtain permission from a classroom teacher or administrator before making publicly available any images, video, or audio files recorded at school.

- Understand that inappropriate use may result in cancellation of permission to use the District's EIS and appropriate disciplinary action up to and including expulsion.

- Understand that many services and products are available for a fee and acknowledge personal responsibility for any expenses incurred without District authorization.

- Use the District-created alias as the only form of masked identity when using the District's EIS.

The following also includes prohibited uses of the District's EIS. Each user of the District's EIS, including a user of a PD, shall not:

- Send, submit, publish, display, or retrieve any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, intimidating, fraudulent, or illegal material.

- Use the network in any way that would disrupt the use of the network by others.

- Use the District's EIS for commercial purposes or personal financial gain.

- Attempt to harm, modify, add or destroy software or hardware nor interfere with system security.

- Disclose home addresses, personal phone numbers or personally identifiable data unless authorized to do so by designated school authorities.

Attempt to log into the District's EIS using any account and/or password other than the login(s) assigned to the user. It is inappropriate to use or attempt to discover another user's password. Sharing of passwords is prohibited. A District employee may use a student account and/or password for troubleshooting purposes only, and should never ask the student for the account information.

In addition, acceptable use for District employees is extended to include requirements to:

- Maintain supervision of students using the District's EIS, including use of PDs.

- Take responsibility for the content of their posting on any form of technology through any form of communication.

- Take responsibility for assigned personal and District accounts, including password protection.

- Take all responsible precautions, including password maintenance and file and directory protection measures, to prevent the use of personal and District accounts and files by unauthorized persons.

- Adhere to all District policies related to technology, including but not limited to, the use of District technology, copyright and trademark laws, student rights, parent rights, the Family Educational Rights and Privacy Act (FERPA), staff ethics, mandatory reporting requirements, and staff-student relations.

Violation of the rules set out above will result in staff and/or student discipline in accordance with state law, Board policies and regulations, the District Code of Conduct, and school handbooks.

Policy IJNDB and this regulation are not intended to prohibit the use of District bulletins on the e-mail system that are for employee personal use only. Currently approved bulletins are "classified ads" and the "advice column."

It shall be the responsibility of all District employees and students to be knowledgeable of the details of the Acceptable Use Agreement. When the signed agreement is returned to the school, the user may be permitted use of the District's EIS resources through the school equipment.

The District reserves the right to enact rules and regulations essential for the efficient administration of the electronic information systems.