IJNDB
USE OF TECHNOLOGY RESOURCES IN INSTRUCTION

Appropriate use of Electronic Information Services

This policy and related regulation and exhibits define the acceptable uses of technology and technological education efforts within the District. The District may provide electronic information services (the District's EIS) to qualified students, teachers, and other personnel who attend or who are employed by the District, or users who acquire access privilege through association with the District. The use of these services shall be in support of instructional, informational, communication, research, administrative, and educational goals of the District.

Electronic information services (EIS) include, but are not limited to networks (e.g., LAN, WAN, Internet), telephone systems/voice mail, electronic mail, databases, hardware, software, Google Apps for Education's G Suite and Additional Services (e.g., Google Docs, Gmail, Google Sheets, Google Classroom), and any computer-accessible source of information. These include, but are not limited to hard drives, tapes, compact disks (CDs), floppy disks, or other electronic sources/media (e.g., Universal Serial Bus [USB] flash drives, iPods), or such similar equipment as may become available.

To assure that the District's EIS is used in an appropriate manner and for the educational purposes intended, the District will require anyone who uses the District's EIS to follow this policy, related regulation, and exhibits for appropriate use. Anyone who misuses, abuses, or chooses not to follow this policy, related regulation, and exhibits will be denied access to the District's EIS and may be subject to disciplinary and/or legal action. This policy applies to qualifying students, employees, and other users who acquire access privileges through association with the District.

The Superintendent shall determine steps, including the use of an Internet filtering mechanism, that must be taken to promote the safety and security of the use of the District's online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. Technology protection measures shall protect against Internet access by both adults and minors to visual depictions that are obscene, child pornography or, with respect to the use of computers by minors, harmful to minors. Safety and security mechanisms shall include online monitoring activities.

It is the policy of the Board to:

- prevent access to or transmission of, inappropriate material via the District's EIS, the Internet, electronic mail, or other forms of direct communications;

- prevent unauthorized access and other unlawful online activity;

- prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and

- comply with the Children's Internet Protection Act [P.L. No. 106-554 and 47USC

254(h)].

Each user will be required to sign an annual EIS Acceptable Use Agreement. The District may log the use of all systems and monitor all system utilization. Accounts may be closed and files may be deleted at any time. The District is not responsible for any service interruptions, changes, or consequences. The District reserves the right to establish rules and regulations as necessary for the efficient operation of the electronic information services.

The District does not assume liability for information retrieved via EIS, nor does it assume any liability for any information lost, damaged, or unavailable due to technical or other difficulties.

Filtering and Internet Safety

As required by the Children's Internet Protection Act, the prevention of inappropriate network usage includes unauthorized access, including "hacking," and other unlawful activities; unauthorized disclosure, use and dissemination of personal identification information regarding minors.

Limits, controls and prohibitions shall be placed on student:

- Access to inappropriate matter.
- Safety and security in direct electronic communications.
- Unauthorized online access or activities.
- Unauthorized disclosure, use and dissemination of personal information.

The protective measures shall also include monitoring the online activities of students.

Circumvention of the District's protective measures is a violation of the Acceptable Use Agreement.

Education, Supervision and Monitoring

It shall be the responsibility of all District employees to be knowledgeable of the Board's policies, regulations, and procedures. Further, it shall be the responsibility of all employees, to the extent prudent to an individual's assignment, to educate, supervise, and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

The Superintendent shall provide for appropriate training for District employees and for students who use the District's computer network and have access to the Internet. Training provided shall be designed to promote the District's commitment to:

- the standards and acceptable use of the District's network and Internet services as set forth in District policy;

- student safety in regards to use of the Internet, appropriate behavior while using, but not limited to, such things as social networking web sites, online opportunities and chat rooms; and cyberbullying awareness and response; and compliance with E-rate requirements of the Children's Internet Protection Act.

While training will be subsequently provided to employees under this policy, the requirements of the policy are effective immediately. Employees will be held to strict compliance with the requirements of this policy and related regulation, regardless of whether training has been given.

The Superintendent is responsible for the implementation of this policy and for establishing and enforcing the District's EIS procedures for appropriate technology protection measures (filters), monitoring, and use. Violations of this policy may result in disciplinary action up to and including termination (in the case of a District employee) or suspension or expulsion (in the case of a student) and may constitute a violation of federal or state law in which case appropriate law enforcement shall be notified. The Superintendent shall report violations of this policy to the Board and shall make reports to the appropriate law enforcement agency when determined necessary.

Acceptable Use Agreements

Each user will be required to sign, annually, an Acceptable Use Agreement. A user who violates the provisions of the agreement will be denied access to the District's EIS and may be subject to disciplinary action.

Parent Notification

Parents will be notified of the policies regarding the use of technology and the Internet while at school. Parents will also be notified of their ability to prohibit the student from the use of technology and the Internet while at school in which covered information may be shared with an operator pursuant to A.R.S. 15-1046. This does not apply to software or technology that is used for the daily operations or administration of a local education agency or Arizona online instruction programs authorized pursuant to A.R.S. 15-808.

Adopted: January 9, 2018

LEGAL REF.:
A.R.S.
13-2316
13-3506.01
13-3509
15-341
15-808
15-1046
34-501
34-502
20 U.S.C. 9134, The Children's Internet Protection Act
47 U.S.C. 254, Communications Act of 1934 (The Children's Internet Protection Act)

CROSS REF.:

GBEA - Staff Ethics
GBEB - Staff Conduct
GBEBB - Staff Conduct With Students
GBEBC - Gifts to and Solicitations by Staff Members
GBI - Staff Participation in Political Activities
GCQF - Discipline, Suspension, and Dismissal of Professional Staff Members
GDQD - Discipline, Suspension, and Dismissal of Support Staff Members
IJM - Interest Materials Selection and Adoption
IMH - Class Interruptions
IMH-R - Class Interruptions
JIH - Interrogations, Searches, and Arrests
JK - Student Discipline
JK-RA - Student Discipline
KHA - Public Solicitations in Schools

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.

Filtering, monitoring and access controls shall be established to:

- Limit access by minors to inappropriate 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.

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. 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 disks 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 and music, streaming music, 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 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/guardian has 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/guardian.

Web Publishing

The District recognizes the value and potential of publishing on the Internet. School faculty and staff are encouraged to create electronic home pages or other pages that seek to carry out official business and communication of the District's mission. All such pages must be accessible to the District, parents, 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/guardian. Staff publishers will be responsible for maintaining their class or educational resource sites. Web pages must reflect positively upon the District and school. Web pages must include an e-mail address of the adult maintaining the page. E-mail addresses/links on web pages must be a cfsdl6.org address. School and teacher websites are the responsibility of the school principal, who designates a school Webmaster. 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/guardian permission.

The Google naming convention will be an alias with first initial, last initial, 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 parents/guardians 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, much the way that students utilize pen and paper. To this end, the District recognizes the value of allowing students 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 to possess and use their PDs at school.

A PD is any electronic device owned by a student or his/her family 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 (iPods or MP3 players), digital cameras, laptop computers, tablet computers, pagers, portable game players, and any new technology developed with similar capabilities.

This regulation applies to a student'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 is permitted to use a PD only after the student and a parent/guardian have signed and returned the annual Acceptable Use Agreement.

- In a classroom setting, a student may only use a PD for educational purposes at the direction of a teacher or administrator. Other than in a classroom setting on school property, the administration at each school will determine where and when and for what purpose a student 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 a classroom setting, a student is prohibited from using a PD to access the Internet using any external Internet service (e.g., 3G/4G connections and mobile hot spots). In a classroom setting, a student using a PD, including a smart phone, 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 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 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 will put the device away and take it home at the end of the school day where the student and the parent/guardian 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/guardian, even if the fees or charges were incurred by the student for an educational purpose.

- A student 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 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 and parents are 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, MySpace, Twitter, YouTube, Instagram, Google+, 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 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, Twitter or other third-party social media requests from students. 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/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, parents, employees, or other members of the school community; or 3) significantly and adversely impact the employee's work-related reputation. 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, parents, 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, parents, 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, parents, and students. 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. 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 Use" of service 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*. A student's personal social media communication can be considered inappropriate 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;

  - involves prohibited discrimination, defamation, harassment, intimidation, threats or bullying;

  - 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. Parents, 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.

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.

- 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.

IJNDB-EA

EXHIBIT

USE OF TECHNOLOGY RESOURCES IN INSTRUCTION

ELECTRONIC INFORMATION SERVICES ACCEPTABLE USE AGREEMENT

(Students and Parent/Guardian)

Students

Sign and return only this Acceptable Use Agreement to the school. Please retain Policy IJNDB and Regulation IJNDB-R for your personal reference.

I have read and will follow District Policy IJNDB and Regulation IJNDB-R. I have specifically reviewed the sections of IJNDB-R regarding the following:

- Student Google Accounts
- Bring Your Own Device (BYOD)
- Use of Social Media by Students
- Search and Seizure
- Acceptable Use

I will also consult the Parent/Student Handbook(s) for any school-specific guidelines. I am responsible for my actions regarding my use of technology. I understand that my use of the District's computer system (referred to as "EIS" in the policy and regulation) will be monitored by the District. I also understand that any violation of Policy IJNDB and Regulation IJNDB-R may result in the loss of District computer privileges and discipline up to and including expulsion.

Parent/Guardian Cosigner

For students under the age of eighteen (18), a parent/guardian must also sign this agreement.

As the parent/guardian of the below named student, I have read District Policy IJNDB and Regulation IJNDB-R and discussed them with my child. I will also consult the Parent/Student Handbook(s) for school-specific guidelines. I accept full responsibility for supervision of my child if, and when, my child uses the District's EIS not in a school setting.

I understand that it is impossible for the District to restrict access to all controversial materials, and I will not hold the District responsible for materials acquired by my child using

the District's EIS. I also understand that the District is not responsible for the accuracy of any information obtained using the District's EIS.

I agree to report any misuse of the District's EIS to a school or District administrator. Misuse may come in many forms, but can be viewed as sending or receiving messages or material that is fraudulent, harassing, sexually explicit, racially offensive, profane, obscene, intimidating, defamatory, unlawful, inappropriate, unethical, or as described in Policy IJNDB and Regulation IJNDB-R.

If I allow my child to bring a personal electronic device (PD) to school, I will not hold the District responsible for any damages to the PD due to theft, loan, damage, or other loss. I understand that I am responsible for the payment of any user fees and/or data charges associated with my child's use of his or her PD that are billed to us by our service provider, even if such fees or charges are incurred in connection with the use of the PD for educational purposes.

I understand that I may prohibit my child's use of technology and the Internet by selecting "NO" below. The child will be prohibited from the use of any district provided electronic information service. This does not apply to software or technology that is used for the daily operations or administration of the district or Arizona Online Instruction programs.

Electronic Information Services' Resources - CHECK ONE:

□ YES, I hereby give my child permission to use the District's EIS Resources at school, including, but not limited to, computers and the Internet, and Google Apps for Education's G Suite and Additional Services.*

□ NO, I do NOT give my child permission to use District's EIS Resources at school, including, but not limited to, computers and the Internet, and Google Apps for Education's G Suite and Additional Services.*

* Google Apps for Education's G Suite and Additional Services has become a standard classroom teaching tool that is integrated within CFSD's K-12 curriculum. This tool is used in many classroom lessons and collaboration activities. If you check "NO," your child will not be able to participate in these planned activities.

Students should understand that their parents/guardians and District staff have the right to access their accounts at any time.

Full Legal Name of Student (printed) _____ Grade _____

Student Signature _____ Date _____

Parent/Guardian Signature _____ Date _____

IJNDB-EB

EXHIBIT

USE OF TECHNOLOGY RESOURCES IN INSTRUCTION

ELECTRONIC INFORMATION SERVICES ACCEPTABLE USE AGREEMENT

(District Employees/Third Parties Associated with District)

Sign and return only this Acceptable Use Agreement to District administration. Please retain Policy IJNDB and Regulation IJNDB-R for your personal reference.

I have read and will follow District Policy IJNDB and Regulation IJNDB-R. I have specifically reviewed the sections of IJNDB-R regarding the following:

- Social Media
- Use of Personal Social Media by District Employees
- Use of School-Related Social Media by District Employees
- Acceptable Use

I am responsible for my actions regarding my use of technology. I understand that my use of the District's EIS will be monitored by the District. I understand that any violation of Policy IJNDB and Regulation IJNDB-R may result in discipline up to and including termination. In addition, I understand that acceptable use for District employees includes requirements to:

- Maintain supervision of students using the District's EIS, including use of personal electronic devices.
- Take responsibility for the content of 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.
- Stay apprised of and 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.

I agree to report any misuse of the District's EIS to a school or District administrator. Misuse may come in many forms, but can be viewed as sending or receiving messages or material that is fraudulent, harassing, sexually explicit, racially offensive, profane, obscene, intimidating, defamatory, unlawful, inappropriate, unethical, or as described in Policy IJNDB and Regulation IJNDB-R.

Employee Name (printed) _____ School _____

Employee Signature _____ Date _____

IJNDB-EC

EXHIBIT

USE OF TECHNOLOGY RESOURCES IN INSTRUCTION

PARENT/GUARDIAN PERMISSION FORM FOR DISCLOSURE OF STUDENT INFORMATION IN CONNECTION WITH ELECTRONICS-BASED TECHNOLOGY IN INSTRUCTION

You are being presented with this form because your student will engage in a class project that meets one (1) or more of the following criteria:

- The project requires the use of personally identifiable information other than District designated directory information.
- Student work is not password-protected from non-District visitors.
- Students are not using the District alias.
- The project requires the use of District e-mail to send to/receive from addresses outside of the District domain.

Your student's teacher is requesting permission for the release of student information other than District designated directory information in connection with the classroom/school-related project or activity described in Section A of the attached Teacher Request/Permission Form. Your authorization for the release of such information is required for one (1) of the following reasons:

(1) Your child's work or project is eligible for publication on a public website that requires the release of student information other than District designated directory information to the website administrator, and/or

(2) The activity or project requires the release or use of student information other than District designated directory information, for educational purposes. Examples of these types of activities may include: presentations and/or competitions that show-case students' writing, artistic or other education-related endeavors; use of personal/home e-mail and/or contact information to facilitate the receipt or transmission of educational research materials; the development and/or presentation of students' digital portfolios; the participation of students in web conferencing with public officials and/or organizations; students' participation in on-line "think tanks" relating to educational topics; and global document sharing.

If you have any additional questions about the project or activity for which your permission is sought, please contact the teacher directly. If you do not wish to grant permission for the release of the student information required in connection with the project or activity described in Section A, the student will be assigned the alternative activity described in Section B of the attached Teacher Request/Permission Form.

Please initial and sign below to indicate whether the District has your permission for the release of student information that is not District designated directory information in connection with the classroom/school-related activity involving the use of electronics-based technology described in Section A of the attached Teacher Request/Permission Form. Please return this form to the teacher prior to the designated proposed start date for the described project/activity.

Note: We cannot accommodate requests for the release of some, but not all, Student Information in relation to the subject project/activity.

Initials _____ I DO grant permission for the District's release of student information that is not District designated directory information in connection with the project/activity described in Section A of the Teacher Request/Permission Form.

Initials _____ I DO NOT grant permission for the District's release of student information that is not District designated directory information in connection with the project/activity described in Section A of the Teacher Request/Permission Form. I understand that my child will be assigned the alternative project/activity described in Section B thereof.

Student Name (Please print) _____

Student Signature _____ Date _____

Parent/Guardian Signature _____ Date _____

I understand that I may withdraw this permission at any time upon my written request to do so.

IJNDB-ED

EXHIBIT

USE OF TECHNOLOGY RESOURCES IN INSTRUCTION

TEACHER REQUEST/PERMISSION FORM DISCLOSURE OF STUDENT INFORMATION IN CONNECTION WITH ELECTRONICS-BASED TECHNOLOGY IN INSTRUCTION

Teacher _____ Date of Request _____

School _____ Grade Level and/or Course Title _____

Proposed Start Date _____ Project End Date _____

The District recognizes the educational and professional value of electronics-based technology, including but not limited to the Internet, electronic mail, hardware, software, and online resources, as a valuable tool that supports teaching and learning through access to resources and information, learning activities, interpersonal communication, research, training and collaboration, and dissemination of successful educational practices, methods and materials. Such technology also provides connections to a wider set of "educators," including teachers, parents, experts/practitioners in the field, and mentors outside of the classroom.

The District supports the use of electronics-based technology that is consistent with the goals of the District while recognizing the need to protect against unauthorized disclosure of information relating to its students. For all electronics-based school or curriculum-related projects or activities that do not require personally identifiable information about students, the District has provided each student with an unidentifiable alias to enable and facilitate the student's participation. There are some electronics-based educational activities that may not allow for the use of such an alias, however.

The teacher is required to seek administrative authorization for any school or curriculum-related project (e.g., publication of student work, digital portfolio, research, online collaboration) involving the use of electronics-based technology that meets one (1) or more of the following criteria:

- The project requires the use of personally identifiable student information that is not District designated directory information.
- Student work is not password-protected from non-District visitors.
- Students will not be using the District alias.
- The project requires the use of District e-mail to send to/receive from addresses outside of the District domain.

The completion of this form by the teacher and the approval of the school administrator (by signing below) are required before the teacher is authorized to seek written permission for disclosure of student information that is not District designated directory information from parents/guardians for participation in the activity.

A. To facilitate an understanding of the project and the manner in which it will utilize electronics-based technology and support the curriculum or otherwise benefit the students, please write a description of the project. The description should include a discussion of the project's use of technology and how the project is expected to reinforce and/or enrich the curriculum (continue on attached sheet of paper, if necessary).

B. Describe the alternative arrangement/assignment you propose for a student whose parent/guardian does not give permission for disclosure of the student information required for participation in the project (continue on attached sheet of paper, if necessary).

Teacher Signature _____ Date _____

Administrator Signature _____ Date_____