STUDENT INTERNET/SOFTWARE ACCEPTABLE USE AGREEMENT

1.0 PURPOSE

1.1 The principal or designee shall oversee the maintenance of each school's technology resources and may establish guidelines and limits on their use. It is the student's personal responsibility to follow the guidelines established in this document and other district policies regarding behavior, bullying, and technology.

2.0. GUIDELINES

2.1. Educational Purpose

The District network has been established as a link to the Internet for educational purposes. This means that students may use the system for classroom activities, professional or career development, and high-quality, educationally enriching research, and other educational activities.

The District may place reasonable restrictions on the material students can access or post through the system, and may revoke access to these resources if there is a violation of the law or this regulation. Violations of the law or this regulation may also be addressed through the District's Student Conduct and Anti- bullying Policy. Violators of the law will be referred to proper law enforcement agencies.

Students may not use the District network for commercial purposes. This means the student may not offer, provide, or purchase products or services through the District network.

The District reserves the right to monitor student activity on district provided devices, networks, and accounts at all times.

2.2. Access to Online Materials

2.2.1. The sites and programs students may access through the District's network will be for class assignments or educational research related to a subject or course of study only. To provide the best possible educational use of the District network, students will be provided access to various educational services which are accessible both at home and at school. These services allow students to access educational content, collaborate on assignments, communicate with peers and teachers, be creative with class assignments, and extend learning opportunities beyond the traditional school day. See your schools website "student links" web page for a list of educational services. Student data (personally identifiable information) will be shared with vendors who agree to follow state and federal laws concerning student data privacy whose programs are deemed necessary for classroom instruction, collaboration, communication, differentiation, or practice

2.2.2. Students will not use the District network or devices to access, publish, send, or receive any material in violation of applicable law. This includes, but is not limited to: material that is obscene; child pornography; material that depicts, or describes in an offensive way, violence, nudity, sex, death, or bodily functions; material that has been designated for adults only; material that promotes or advocates illegal activities; material that promotes the use of alcohol or tobacco or weapons; material that advocates participation in hate groups or other potentially dangerous groups; materials that promote illegal behavior; material protected as a trade secret or material that can be

construed as harassment or disparagement of others based on their race/ethnicity, gender, sexual orientation, age, disability, religion, or political beliefs.

2.2.3. Students who mistakenly access inappropriate information must immediately report such access to a teacher or other staff member. Timely reporting of this material may help to protect a student against a claim that he/she has intentionally violated this regulation.

2.2.4. Staff shall supervise students while they are using online services and may have teacher aides, student aides, and volunteers assist with supervision. Parent/Guardian is exclusively responsible for monitoring his or her child(s) use of the Internet when off campus and when accessing District approved online educational systems from home or a non-school location. The District does not employ its filtering systems to screen home access to the District online educational systems.

2.2.5. Students' in grade kindergarten through twelve will be issued Google Application accounts in the District Google educational domain. Google Applications is a service provided by Google that allows users to effectively communicate and collaborate in a safe and secure online educational environment while increasing organization and preventing lost homework as all work is stored in the Google Server Cloud. The District Google domain is managed and secured by district administrative oversight. The district has the right to monitor and archive all student activity in the Google domain. Google Applications enable students to log into their accounts to work from any Internet connected device. Students can only interact with District students and staff within the domain, unless the student purposefully shares their work with a user outside the domain. Students shall not share their work with anyone outside the District domain or invite others outside the District domain unless given express permission by their teacher or site administrator. Students shall only share and collaborate on projects that have been assigned by a teacher. Students will respect the collaborative work of teachers and peers

2.3. Protection of Personally Identifiable & Confidential Information

2.3.1. To protect one's personal contact information, students will not share online their full name or information that would allow an individual to locate a student, including family name, home address or location, work address or location, or phone number. Students will not disclose names, personal contact information, or any other private or personal information about other students or District employees. If personal information is shared, students will promptly disclose this to their teacher or school administrator. Any message one receives that is inappropriate or makes them feel uncomfortable should be reported as well. Students should not delete such messages until instructed to do so by a school staff member.

2.3.2. The Family Educational Rights and Privacy Act ("FERPA") prohibits school officials from disclosing personally identifiable information ("PII") from education records of students and families to third parties without parental consent. Personally identifiable information includes but is not limited to student name, school assigned student identification number, email address, phone number, ethnicity, and grade level. Exceptions to this general rule may apply when releasing PII to online education

learning solutions. The District releases student information to approved online educational solutions to enhance the learning process. The district approved online educational providers agree to and comply with District information security regulations in order to protect the transfer and storage of personal identifiable information to the third-party provider. No third-party disclosure of PII is acceptable. The provider may not use data to target ads towards the student.

2.4. Unlawful, Unauthorized, and Inappropriate Uses and Activities

The following activities are unlawful, unauthorized, and inappropriate:

2.4.1. Attempting to gain unauthorized access to the District network or to any other computer system through the District network or go beyond your authorized access. This includes attempting to log in through another person's account or to access another person's files.

2.4.2. Students will not connect any personal devices to the District network, other than the District guest network, without express permission from the District's Technology Department. Guest access to the District's guest wireless network is provided as a service to the community and is subject to all policies and guidelines covered in this agreement. This includes, but is not limited to smartphones, eReaders, smart-watches, and Personal Computing Devices (see section 2.12 for more information on guest network access)

2.4.3. Making deliberate attempts to disrupt the District network or any other computer system or destroy data by spreading computer viruses or by any other means.

2.4.4. Using the District network to engage in any other unlawful act, including arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, or threatening the safety of any person.

2.4.5. Attempting to alter or interfere with other users' abilities to post, send, receive, or submit material.

2.4.6. Attempting to delete, copy, or modify another users' work, or identity.

2.4.7. Creating a personal network or "hot spot" with unauthorized equipment in order to gain access to the District Internet. Utilizing proxies, personal networks, or cellular networks or hot spots in order to bypass the district filter.

2.4.8. Utilizing peer-to-peer file sharing, torrents, or similar technology to download, steal, copy, or borrow copyrighted work, music, video, movies, or other content.

2.4.9. Using the District network to cheat.

2.5. Inappropriate Material and Language

Students must avoid inappropriate language in their electronic communications. Students will not:

2.5.1. Use obscene, profane, lewd, vulgar, inflammatory or threatening language or images including but not limited to "sexting", "zoombombing", or disruption of

class during video conferencing.

2.5.2. Post information that may cause damage or a danger of disruption to your school or any other organization(s) or person(s) without written consent of administration/designee.

2.5.3. Post photographs, video, or voice recordings of any person(s) of any person(s) without the consent of administration/designee or the written consent of any adult(s).

2.5.4. Engage in personal attacks, including prejudicial or discriminatory attacks.

2.5.5. Harass or bully another person. Cyberbullying is prohibited by state law and district policy. Bullying or harassment that is done on or off campus, at any time, with a computer or any type of communications device may result in discipline at school up to and including expulsion, legal action, or prosecution by the appropriate law enforcement authorities.

2.5.6. Knowingly or recklessly post false or defamatory information about a person or organization.

2.5.7. Students will promptly disclose to a teacher or another school employee any message they receive from any other student that is in violation of the restrictions on inappropriate language. Students will not delete these messages until instructed to do so by an administrator.

2.6. Plagiarism and Copyright Infringement

Students will not plagiarize works that they find on the Internet. The definition of plagiarism is taking the ideas or writings of others and presenting them as if they were your own.

Students will respect the rights of copyright owners in their use of materials found on, disseminated through, or posted to the Internet. Copyright infringement occurs when students inappropriately reproduce or share a work that is protected by a copyright. Students may not quote from any source without proper attribution and/or permission. Students may not make or share copies of copyrighted songs or albums, digital images, movies or other artistic works. Unlawful peer-to-peer network file-sharing may be a criminal offense. Copyrighted material may not be placed on the District system without the author's permission. Students may download copyrighted material for their own use only under "fair use" provisions of the copyright law. See http://www.loc.gov/teachers/copyrightmystery/#

2.7. System Security and Resource Limits

Security on computer systems is a high priority. At all times, students are required to use their District provided individual account. Students are responsible for their individual account and should take all reasonable precautions to prevent others from being able to use their account. Under no conditions should students provide their password to another person. Students will immediately notify a teacher or other staff member if they have identified a possible security problem.

If students identify a security problem, they should notify the teacher or other staff member at

once. Students should never demonstrate the problem to others.

Students will not download large files unless absolutely necessary. Students will not misuse district, school, or personal distribution lists or discussion groups for sending irrelevant messages

2.8. No Reasonable Expectation of Privacy

Students should not expect privacy in the contents of their personal files on the District network, District approved cloud storage systems, District devices, and records of their online activity. The District's monitoring of Internet usage can reveal all activities students engage in using the District network and devices. Students will not attempt to change their District-assigned password on any program, unless authorized by the technology department.

Maintenance and monitoring of the District network may lead to discovery that students have violated this regulation, the student conduct policy, or the law. An individual search will be conducted if there is reasonable suspicion that a student violated this regulation, the student Conduct Policy, or the law. The investigation will be reasonable and related to the suspected violation.

Parents have the right to request to see the contents of their student's computer files at any time as it relates to FERPA.

2.9. Vandalism

Vandalism, in addition to physical damage, is also defined as any malicious attempt to access, harm, alter, or destroy data of another user or any other agencies or networks that are connected to the system. This includes, but is not limited to, the uploading or creation of computer viruses or hacking. Any vandalism may result in the loss of computer services, disciplinary action, and/or legal referral.

2.10. Video Conferencing

Video conferencing allows for synchronous teaching and learning of material through a platform such as Zoom, Google Meet, or other platform. Video conferencing is instructional time and an extension of the physical classroom. Behavior on a video conferencing platform must conform with student classroom expectations and the student discipline handbook. Students may not record or distribute video conference meetings without the written consent of the teacher or administrator in accordance with Administrative Regulation 6.14 (https://drive.google.com/file/d/0B7no0GfL-TcgVTkzbl9yaXVIaDQ/view)

2.11. Violations of this Regulation

The District will cooperate fully with local, state, or federal officials in any investigation related to any unlawful activities conducted through the District electronic infrastructure to include Internet and network access; e-mail, grading systems, databases and user accounts.

In the event there is a substantiated claim that a student has violated the law, this regulation, or the District's student conduct policy in the student's use of the District network, the student's access to the District's computer resources may be terminated and/or the student may be disciplined under applicable District policies or referred to law enforcement as

applicable.

2.12. Responsibility for Loss or Damages

Parents can be held financially responsible for any harm that may result from a student's intentional misuse of devices, accounts, or network.

The District assumes no responsibility for the loss, destruction or theft of any personal devices including but not limited to cellular phones, computers, or personal electronic devices. Devices should not be left unattended. School officials and District office staff are not required to investigate lost or stolen personal electronic equipment.

The District is not responsible for online material accessed off campus on a non-District network.

If a District-purchased device is checked out to a student with written parent permission for use off campus, parents can be held financially responsible for loss or damage to the device.

2.13. Personal Mobile Devices

The Superintendent or designee shall make available to all students the opportunity to connect an approved personal technological device to the District provided guest wireless network for academic purposes. Students using their own device to connect to the guest wireless network must do so with their District issued individual account. If applicable, the personal device must have current anti-virus and anti-malware software installed before accessing the network. The device may be used in the classroom or learning space for academic purposes only. The individual school site may provide direction on expectations of utilization and device specifications, with guidance from the technology department and legal.

The Superintendent or designee shall establish guidelines for schools to implement "Bring Your Own Device" programs or "1 to 1 Device Checkout" programs with clear procedures on ensuring equity of access and compliance with Education Code 49011, prohibiting required student fees to participate in an educational activity.

The use of personal mobile devices, such as laptops, Smartphones, tablets, etc., by students on campus is subject to all applicable District policies and regulations concerning technology use. The use of district devices, such as laptops and hotspots, by students at home are subject to all applicable District policies and regulations concerning technology use. In addition, the following rules and understandings apply:

2.12.1. Permission to have a mobile device at school is contingent upon parent/guardian understanding this agreement except as required by Education Code section 48901.5(b)

2.12.2. All costs for data plans and fees associated with personal mobile devices are the responsibility of the student. The District does not require the use of personal mobile devices in any instructional setting but may allow their use to enhance learning.

2.12.3. Schools supporting subject or grade level programs where students participate in a Bring Your Own Device program will provide equity devices, equivalent to the

current District standard, to ensure everyone has the opportunity to participate.

2.12.4. Mobile devices with Internet access capabilities which are being harnessed for classroom learning purposes are required to use the District filtered wireless network.

2.12.5. Students are required to use their District issued individual account to access the wireless network at all times.

2.12.6. Use during class time must be authorized by the teacher.

2.12.7. Students are directed not to photograph, video tape, or record any individuals without the explicit permission of the teacher or administrator. Recordings made in a classroom require the advance permission of the teacher or school principal.

2.12.8. Students may not take, possess or share obscene photographs or videos.

2.12.9. Students may not photograph, videotape or otherwise record instructional materials and assessments.

2.12.10. The District assumes no responsibility for the loss, destruction or theft of any personal devices including, but not limited to, cellular phones, computers, or personal electronic devices. Devices should not be left unattended. School officials and District office staff are not required to investigate lost or stolen personal electronic equipment.

2.12.11. The District is not responsible for online material accessed off campus on a non-District network.

2.12.12. Students should not expect privacy in the contents of their personal files on the District network, District approved cloud storage systems, District devices, District accounts, and records of their online activity. The District's can monitor student Internet usage. Parents have the right to request to see the contents of their student’s computer files at any time.

2.12.13. Staff shall supervise students while they are using online services and may have teacher aides, student aides, and volunteers assist with supervision. Parent/Guardian is exclusively responsible for monitoring his or her child(s) use of the Internet when off campus and when accessing District approved online educational systems from home or a non-school location. The District does not employ its filtering systems to screen home access to the District’s online educational systems.

2.12.14. Cyberbullying is prohibited by state law and District policy. Bullying or harassment that is done on or off campus with a computer or any type of communications device may result in discipline at school up to and including expulsion, legal action, or prosecution by the appropriate law enforcement authorities.

2.12.15. It will be each student’s responsibility to follow the rules for appropriate and responsible use as detailed in the Student Internet/Software Acceptable Use Agreement. Access to the wireless network and access to a District device is a privilege and administrators and staff may review files and messages to maintain

system integrity and ensure that users are acting responsibly. The District is not responsible for theft, loss, or damage to personal technology devices that are brought to school from home by students.

2.13. District-Owned Mobile Devices

When a student is using a District-owned mobile device, all of the above rules pertaining to personal mobile devices apply, as well as the following:

2.13.1. The device may be used only for school-related purposes.

2.13.2. Users may not download applications ("apps") to the device without permission from the teacher.

2.13.3. For PC, iOS, and Android tablets/mobile devices, software apps may only be loaded with teacher or other District employee permission.

2.13.4. For Chromebooks, students may add educationally appropriate "apps".

2.13.5. Users must follow all "apps" use agreements. The student and parent/guardian will be responsible for the replacement cost if the device and/or accessories are lost, stolen, or is damaged.

3.0 ACTION

The principal or designee may cancel a student's user privileges whenever the student is found to have violated Board policy, administrative regulation, or the District's Student Acceptable Use Agreement. Inappropriate use may also result in disciplinary action and/or legal action, which may include suspension, expulsion, or referral to law enforcement in accordance with law, school and Board policy.

Administrative Regulation CAPISTRANO UNIFIED SCHOOL DISTRICT

Approved: (4/08) San Juan Capistrano, California
Revised: (8/09)
Revised: (8/11)
Revised: (5/12)
Revised: (7/15)
Revised: (6/18)
Revised: (7/20)

STUDENT INTERNET/SOFTWARE ACCEPTABLE USE AGREEMENT

Capistrano Unified School District provides students with access to digital devices, accounts and the Internet through the District network to teach the adopted curriculum and prepare students to meet the challenges of a rapidly changing world. Students are responsible for the rules and regulations of the Student Internet/Software Acceptable Use Agreement, summarized below. For the entire regulation document that must be followed while a student at CUSD, please read the entire Administrative Regulation 6.7 available on the Parent Portal and included in the document read as part of the annual data confirmation before school started. Students not returning this document signed by student and parent will be removed from technology use during the 3rd week of school. Usage Guidelines:

- Students are given a district and Google account in the District domain to help with authoring documents and presentations, collaboration, and research.
- Students are responsible for maintaining the privacy of their username and password. Students should notify a teacher if they feel their account has been compromised.
- Students may only connect to the Internet through the District provided wireless network while on campus including personal cell phone data plans, mifi devices, or other personal plans.
- Students agree to access computers through their account only.
- Students agree to respectful interactions with other users including their connectivity, access, belongings, accounts, intellectual property, collaboration, and communications.
- Students agree to utilize the District account to generate content that is relevant to curriculum, respectful of others, and responsibly curate, present, and distribute information keeping in mind copyright and intellectual property laws.
- Students must acquire permission before taking, storing, or posting images or videos of other students or staff members.
- Use of personal devices on CUSD campuses is at the discretion of site administration.
- The District protects the students' personally identifiable information; requiring vendors to comply with all state and federal laws (i.e. FERPA, COPPA, etc) concerning student data privacy.
- All files created using the district accounts are accessible to parents and district employees.
- Parents are responsible for intentional misuse and destruction of district devices and all personal devices.

Students found in violation of any board policy and/or administrative regulation may be subject to disciplinary action, financial responsibility, and/or referral to law enforcement

Parent/Guardian Name	Student Name	Date
_____	_____	_____
Parent/Guardian Signature	Student Signature	
_____	_____	