Parent or Legal Guardian: Read this document carefully and work with us in helping your student understand and abide by the rules outlined in this Responsible Use Policy.

Purpose

The Colton Joint Unified School District (CJUSD) believes in the educational value of using instructional technology and recognizes the potential of such to support curriculum and student learning. Our goal in providing electronic resources is to promote academic excellence by facilitating resource sharing, innovation, and communication. We will make every effort to protect students from any misuses or abuses as a result of their experiences with an information service.

21st Century Learner

Technology is an integral part of our students' lives and futures, and we strive to provide technology rich learning environment for students. Students need to learn and master the technology skills necessary to succeed in the technological 21st century global society. However, inappropriate use of these resources may result in disciplinary action and/or referral to legal authorities. The site administrator, district administrator, and/or systems administrator may limit, suspend, or revoke access to technology if deemed necessary.

Filtering and Monitoring

As required by the Federal Children's Internet Protection Act (CIPA), content filtering technology is used to restrict access to unacceptable materials on all Internet access provided by CJUSD. The district makes every effort to limit access to objectionable material; however, no web filtering is 100% safe. With internet access a risk exists that students may access material that may not be of educational value in the school setting. Students who intentionally access, publish, or attempt to access or publish inappropriate or illegal material or Internet sites, may be subject to discipline; which may include the possibility of suspension or expulsion.

If a student identifies a security problem, they are required to notify a teacher or administrator at once, and not demonstrate the problem to other users. Students should also never use another individual's account. All use of the system must be under your own account. If a user is identified as a security risk, he or she may be denied access to the information system and face potential disciplinary consequences.

Individualized Learning Resources

Students may participate in online environments related to curricular projects or school activities and use digital tools, such as, but not limited to, mobile devices, blogs, discussion forums, RSS feeds, podcasts, wikis, and online meeting sessions. In providing educational materials—such as a learning management system to provide individualized instruction based on student ability determined by student input—these resources may collect students' personally identifiable information. Parents/guardians will be deemed to have given consent for students under the age of 13 to access such educational resources, unless the parent/guardian affirmatively opts out of allowing student access to the educational program. To opt a student under the age of 13 out of access to online educational resources that may collect personally identifiable information, parents/guardians should contact the site principal to process this request.

No Expectation of Privacy

The use of CJUSD owned information technology is not private. Students must understand that there is no implied right to privacy when using the district system. All electronic communications and

downloaded material, including files deleted from a user's account, may be reviewed by district officials to ensure proper use of the system. CJUSD has the right to monitor, inspect, copy, review and store any and all usage of CJUSD technology resources including transmitted and received information at any time and without prior notice.

Digital Citizenship

Access is an academically important privilege that entails responsibility. While utilizing CJUSD network and educational technology resources, students are expected to exhibit responsible behavior and refrain from engaging in inappropriate use.

The use of any of CJUSD's electronic information resources should be in support of education and research, having the educational goals and objectives of the Colton Joint Unified School District in order to further the education of students. Technology provided by CJUSD will be used by the student primarily for pursuing and promoting knowledge about the lessons and units teachers assign as part of the teacher's regular curricula. Students are personally responsible for this provision at all times when using electronic information resources.

When using any District electronic resource, students are expected to comply with all District policies, regulations and any applicable laws. The following are some of the electronic resources made available to CJUSD students.

> Email - Students are issued electronic mail from the CJUSD network, and it should be used for educational purposes only and under the direction of a teacher or administrator. Students will in no way use email to spread rumors, gossip, or engage in activity that is harmful to others. Students should not give out their email address unless instructed to do so from a teacher or administrator.

> Cloud Computing - We have experienced a shift in technology from software that resides on servers and computers to applications that reside on the internet or in the cloud. As of 2013, CJUSD has adopted Google Apps For Education as its primary student productivity and communication software. Students need to understand how to safely use these applications. Students must follow the direction and rules outlined by their teacher and/or administrator when cloud computing. More information about Google's privacy and data polices and be found here: https://www.google.com/edu/trust/

> Learning Management System - Learning Management Systems (such as Haiku Learning and/or Google Classroom) will be used by students to access teacher created lessons, tests, discussions, assignments, calendars, wikis, grades, and other classroom resources. More information about Haiku Learning's privacy and data polices and be found here: https://support.haikulearning.com/hc/en-us/articles/202577843-Privacy-and-Security

> Web 2.0 Tools - Web 2.0 tools will be used for creating projects and presentations, peer editing, creative writing, sharing, discussions, research, collaborating, and communicating.

> Communication and Social Media - Students may use blogs, discussion boards, messaging, and/or social media in a moderated environment established to support educational purposes under the direction of a teacher or administrator. These tools and services are accessible via the internet and may be intended for a global audience. While using these communication tools and social media, students must adhere to all aspects of this Responsible Use Policy. Students should

2

not use these communication tools and social media sites for personal use or without direction from a teacher or administrator.

Cyber/Personal Safety - Students are responsible for their individual accounts and should take all precautions to prevent others from being able to use them, which includes but is not limited to keeping passwords private. Students should never share their user name/passwords with other students or log-in under another student's name and/or trespass in other student's files. Students should not share personal information about themselves or others over the internet. Students should not agree to meet with anyone they have met online, and should notify a teacher or other school employee if they receive any message that is inappropriate or makes them feel uncomfortable.

Netiquette - Students should always use the Internet, network resources, and online sites in a courteous and respectful manner. Students should also recognize that an abundance of the valuable content online is often unverified, incorrect, or inappropriate. Students should use trusted sources when conducting research via the Internet. Students should also remember not to post anything online that they wouldn't want parents, teachers, or future colleges or employers to see. Verbal or written language that is considered inappropriate in the classroom is also inappropriate online. Once something is online it can be shared and spread in ways never intended.

Unacceptable Use, Violations

Students must understand that all rules of conduct described in the School Handbook also apply when using technology resources. Unacceptable use can come in many forms, but it is commonly considered as the viewing of any website and/or any message(s) sent or received that indicate or suggest pornography, unethical or illegal activity, racism, sexism, inappropriate language, threats, intimidation, sexual harassment and/or bullying of any individual or groups and other issues further described within this document.

Students should report any misuse of CJUSD technology resources (electronic resources) to administration.

Violation of District Policies, Regulations and/or laws, including but not limited to California Education Code 48900 subdivisions related to improper conduct or misuse of District property, including hardware or cloud-based content, even if not expressly defined herein, may lead to disciplinary action including loss of computer, network and/or internet and e-mail privileges suspension, expulsion, or prosecution when appropriate.

Web Access/Internet/Network – Students shall not attempt or gain unauthorized access to the network or District blocked sites. Students will not use the network or internet for any type of activity or personal gain.

Copyright/Plagiarism – Students will not violate copyright laws or software licensing agreements. Plagiarism is the act of using someone else's words or ideas as your own. Students will not copy materials without the permission of the author and must properly cite all information acquired through the internet or other information technologies. Plagiarism of internet resources will be treated in the same manner as any other incidences of plagiarism.

Cyberbullying – Cyberbullying will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyberstalking are all examples of cyberbullying. Students should never send, or encourage others to send, abusive messages. Students who send emails or post comments with the intent of scaring, hurting, or intimidating others will receive severe disciplinary action and loss of privileges. In addition, students should never post pictures, information or work of other students without their permission. Students should understand that instances of Cyberbullying created when not at school or after school hours can result in disciplinary action at school.

Vandalism – Vandalism is defined as any malicious attempt to harm or destroy property, including data of another user or system on the network or the internet. This includes, but is not limited to, uploading or creating computer viruses, and any attempt to disrupt network services. Vandalism includes any activity that can be described as hacking, cracking, passwords, sending junk or unwanted e-mail (SPAM). Vandalism also includes the intentional damage of computer hardware, peripherals, and software media. Any vandalism will result in the loss of computer services, disciplinary action, and legal referral including suspension and/or expulsion, and the immediate loss of access to the system. Parents may be liable for the cost of the damage that students cause to school property.

Software – Software is available to students to be used as an educational resource. Students should not load or modify software without the consent of an administrator.
Hardware – Hardware and peripherals are provided as tools for student educational purposes. Students are not permitted to install or relocate network hardware and/or peripherals (except for portable devices), or to modify settings to equipment without the consent of the District Information Technology Department.

BYOD (Bring Your Own Device) – CJUSD may provide access for students to the internet on their own electronic devices. The student is fully responsible, at all times, for the personally owned device brought to school and should follow all the rules outlined in this Responsible Use policy. Students who utilize their own devices on campus will be deemed an authorized user of the device by the District and may be required to grant the District access to the device in the event there is a reasonable suspicion of wrongdoing and/or for the teacher to access student work product in conjunction with curriculum and instruction.

Student Photos

The District may share photos of students in a variety of mediums—including but not limited to the school newspaper, school or District website or social media page—to highlight academic achievements, athletic accomplishments, or otherwise promote the District. Should a parent or guardian wish to exclude their student's photo from being shared, please contact the site principal to complete a photo opt-out form.

Student Responsible Use Pledge

Colton Joint Unified School District provides computers, Internet access, and other technology resources for educational use. In accepting the responsibility of being issued access to CJUSD technology resources, students are expected to abide by the following pledge:

As a student, I will practice good digital citizenship when using these technology resources. Good digital citizenship is good citizenship. I understand that I must act appropriately and follow these rules in order to be a good digital citizen, and I realize that I can be disciplined if I do not follow these guidelines and use computers and the Internet inappropriately.

Respect and Protect Myself

➢ I understand that school computer files, email, and internet use are not private and can be monitored by teachers or administrators.
➢ I understand that I must not give my password or username to anyone and will not use others' usernames and passwords.
➢ It is my responsibility to stay safe on the internet. I will not share personal information about myself or others like: home address, phone numbers, passwords, personal photos, or Social Security numbers. I will not meet with anyone met on the Internet and tell parents, teachers, or administrators immediately if someone asks to meet you.
➢ I will not attempt to access profane or obscene material. If I do so accidently, I will not share it with other students and will notify a teacher or administrator right away

Respect and Protect Others

➢ I will use the computer and Internet only with teacher permission and for the purpose that the teacher requested
➢ I will respect copyright laws, not copy material without permission, and I will make sure to show where I found my information
➢ I will be polite and show respect and never cyberbully others. I will not harass, insult, or attack others.
➢ I will not send or display offensive messages or pictures, or use obscene language in messages.

Respect and Protect Property

➢ I will respect and take good care of devices/equipment and technology resources I use.