Exhibit
Student Use of Technology

E 6163.4
Instruction

STUDENT TECHNOLOGY ACCEPTABLE USE POLICY
AND RELEASE OF DISTRICT FROM LIABILITY

Lake Tahoe Unified School District offers its educational community offer a wide range of technologies to support teaching and learning. The district aims to promote a learning environment that is respectful, secure, and responsible. This Technology Acceptable Use Policy provides students guidelines as to how this can be carried out in a digital context.

Use of district technology resources shall comply with federal and state laws and in accordance with the policies and procedures of LTUSD. This Student Technology Acceptable Use Policy also applies per California Education Code 48900 which describes a school's jurisdiction over student activity and discipline to include:

1. *While on school grounds.*
2. *While going to or coming from school.*
3. *During the lunch period whether on or off the campus.*
4. *During, or while going to or coming from, a school-sponsored activity.*

The advent of online learning spaces, particularly those managed by the school district (including Google's G-Suite) expands the concept of class time beyond the school campus. In fact, students may consider their use of district provided online accounts a school-sponsored activity so that their actions and behaviors while online using school accounts and interacting with their classmates do fall under the purview of this Acceptable Use Policy.

District technology includes, but is not limited to, District owned and/or district managed computing devices and peripherals (e.g., computers, laptops, tablets, removable storage devices, wearable technology, interactive classroom projection systems, etc.) District network and communication devices/services (telephones, wired and wireless networks including WiFi access points, emergency radios, email systems, file servers, etc.), and District managed online services (such as G-Suite, Aeries, etc.); access to online information sources; and future technological innovations.

Failure to adhere to this policy may result in discipline including loss of access, confiscation of a device, or up to and including expulsion in accordance with the student behavior and discipline policies. Students are expected to practice ethical behavior when using District and personal technology tools in all areas while refraining from harassment, academic dishonesty, and plagiarism. At the discretion of the school site, District administration, or in accordance with law, students may be disciplined for engaging in conduct deemed detrimental to the school and its mission, or harmful to other students. All aspects of this acceptable use policy apply whether

District technology is accessed on or off campus and whether through District-owned or personally-owned devices. By using District managed technology tools and services, students and parents agree to the following stipulations:

1. By using District technology tools and services whether from personal or District-owned devices, students and parents grant specific consent, as defined by the California Electronic Communications Privacy Act (also known as Senate Bill 178), to the District to review and monitor all electronic communication information and electronic device information created with, stored on, or transmitted via District technology services.

2. Students and Parents acknowledge that the district may therefore monitor or access any and all student use of District technology without further specific advanced notice and that they have no expectation of any right to privacy while using district devices or network services, which includes, but is not limited to, any and all files and communications traveling over or stored on its network, or while using District provisioned accounts and online resources including email and online collaboration tools at any time.

3. Students agree to abide by the school's policies at all times, especially when using District technology tools and services. Students and Parents agree that any inappropriate use of technology while on campus or through district managed accounts off campus may result in school discipline.

4. Students understand that electronic devices are only permitted for educational uses while on campus. Students who play games, text message, or attempt to access social networking websites or applications during class time without the direction and supervision of a teacher may have the privilege to use District technology suspended or revoked. Repeated violations may result in more severe consequences

5. Parents agree that the district may act as an authorized agent for the creation of student online accounts solely for educational purposes in accordance to state and federal student information privacy laws (COPPA, FERPA, SOPIPIA, etc.). District managed student accounts may include, but are not limited to, online accounts created to access Google G-Suite (Google Apps for Education) and access to other apps, programs, or online services and digital curriculum resources.

6. The District holds the safety of its students in highest regard. However, the ability to share information and teach responsible digital citizenship is also vital to the educational process. This includes the use of e-mail, school learning management systems, online collaboration tools, classroom photo sharing services, and other social media avenues when applicable.

7. Parents and students understand that cellular phones and personal electronic devices outside of the district's managed 1-to-1 computer program may be brought to campus and used only under specific circumstances. Students who bring personal electronic devices to campus do so at their own risk and release the District from liability due to loss, damage, or theft of device, or loss of use of the device if confiscated. During class time, these devices may only be used under the direct supervision and instruction of a teacher or administrator. Individual school sites may enforce restrictions or rules regarding electronic device use in addition to the prohibitions below.

The following activities or uses of technology are strictly prohibited to ensure a respectful digital learning environment:

- Using technology to threaten, bully, or harass others. This may include, but is not limited to, sending, accessing, uploading, downloading, or distributing text, images, or other materials that are offensive, threatening, profane, obscene, or sexually suggestive.

- Recording video or audio of other students or staff without their permission.

- Searching for, accessing, or possessing lewd, sexually suggestive, graphically violent, or derogatory/demeaning images and/or media files.

- Using District issued devices or network to search for and/or access repositories of illegal content, content that may cause harm to the District's network, or content that promotes, encourages, or teaches students how to commit an illegal act (i.e. bomb making, pirating electronic media, intentionally causing harm, etc.).

- Bypassing (or attempting to bypass) the District's internet content filter through a web proxy, anonymizers, or other means from a District or personal computing device.

- Circumventing network security measures or attempting to access confidential, private, or restricted information on the District's network or district managed online services.

- Sharing one's passwords or access to online accounts with anyone other than the student's parent or trusted adult.

- Logging into a device or service with the account of another student or a staff member or otherwise gaining access to their files and accounts without their permission.

- Sharing, publishing, or otherwise distributing confidential personal identification information, such as the name, home address, telephone number, Social Security number, financial details, or login credentials and passwords, of another student, staff member, or other person, with the intent to threaten, intimidate, harass, or harm that person.

- Destroying, damaging, defacing, or rendering unusable any property (both physical property like a computer, or virtual, such as a webpage) belonging to the District or another student or adult.

- Altering a district device's settings in a manner to cause confusion, frustration, or loss of use to other users (changing backgrounds, homepages, dock, network configurations, account logins, etc.).

- Using or installing viruses, malware, keyloggers, spyware, or other software/hardware that can be used to damage the District's network, harvest other users' login information, or propagate unwanted messages or files.

- Illegally downloading, storing, installing, or transmitting copyrighted materials without the proper license or permissions. The district explicitly forbids student use of torrenting software or services on the District network.

- Stealing others' intellectual property including text, music, movies, and software, or using them without the appropriate citation or expressed permission in accordance with Copyright Laws and Fair Use guidelines.

- Visiting social networking sites that are not directly used for educational purposes (including Facebook, Instagram, Twitter, Vine, etc.) during class time.

- Use of instant messaging or chat rooms not directly related to instruction (including texting, picture messaging, audio and video messaging) during class time.

Permanent Digital Footprint

Students are reminded that anything they put online creates a permanent digital footprint that remains out of their control. Be mindful that the digital trail one creates for themselves and others is more like a tattoo which is almost impossible to completely erase. Apps, websites and software that claim to delete information may still leave a permanent record accessible to others. Students should not assume their online presence will remain private and should conduct themselves online expecting that any and all data they furnish could be accessible to a wider audience such as admissions officers and potential employers in the future.

Student Online Accounts and Opting Out

As the District works to fulfill its mission of preparing students for the work force they will soon be entering, it will increasingly utilize tools and resources that are housed online and accessed through the internet. Online accounts are necessary to access web based file storage and collaboration tools such as Google Drive, Google Classroom, Google Docs, and District administered Google email as well as other educational web resources. These web and cloud based services permit online distribution and hand-in of student assignments, online based class

discussions and collaboration activities, web based curriculum or learning resources, and in some grade levels, student email.

All District provisioned student accounts will be in compliance with state and federal student privacy requirements. In California, the Student Online Personal Information Protection Act SOPIPA (AB1584, SB1777, and AB1442) creates privacy standards for all online services catering to K-12 education in California and prevents them from advertising to students, building digital profiles about them, and/or selling harvested student information to other parties. The District believes these restrictions provide a safe environment for students to utilize accounts that are created by the District for accessing online educational resources and services.

The federal Child Online Privacy and Protection Act (COPPA) allows Local Education Authorities (LEA's) such as districts and schools to provide consent on the parent's behalf to create online accounts which may collect student information limited to the educational context and for no other commercial purpose. LTUSD operates under COPPA guidelines to create and manage student online accounts. By law, parents may choose to have their child opt out of this implied parental consent. This may be done in LTUSD by obtaining the Student Online Account Opt-Out Form from the school office, scheduling a conference with the school principal, and completing and signing the Opt-Out form in the presence of the principal who will counter sign receipt of the form after a discussion about the reasons for and the consequences of opting out.

Opting out of District managed online accounts for students would significantly impact a child's ability to participate in many class lessons and activities and would prevent students from learning state mandated digital citizenship principles and practicing responsible digital behaviors being taught in class. It might make it difficult for them to receive assignments, participate in online collaborative class projects, submit work back to their teacher, or access online lessons, digital textbooks, and online tutorials. Because the district's progressive use of technology to enhance learning is part of its core values, virtually all parents recognize the importance of allowing the district to carry out its mission to promote responsible digital citizenship and safe online practices and behaviors for all students though creating and maintaining student online accounts.

As part of the student's graduated digital citizenship training strategy students in grades K-8 will have limited email functionality which only allows them to send and receive emails with their teacher and other students within the District, but not the "outside world". Students in higher grades (9-12) may be granted more access to send and receive emails with individuals and organizations outside of the District as needed, but all email communications may be monitored by the District.

Student Name: _____

School: _____ **Grade:** _____ **Student ID:** _____

Student Acknowledgment
I have received, read, understand, and agree to abide by this Acceptable Use Agreement and other applicable laws and district policies and regulations governing the use of district technology. I understand that there is no expectation of privacy when using district technology. I further understand that any violation may result in loss of user privileges, disciplinary action, and/or appropriate legal action.

Name: _____ Grade: _____
(Please print)

Signature: _____ Date: _____

Parent or Legal Guardian Acknowledgment
If the student is under 18 years of age, a parent/guardian must also read and sign the agreement.

As the parent/guardian of the above-named student, I have read, understand, and agree that my child shall comply with the terms of the Acceptable Use Agreement. By signing this Agreement, I give permission for my child to use district technology and/or to access the school's computer network and the Internet. I understand that, despite the district's best efforts, it is impossible for the school to restrict access to all offensive and controversial materials. I agree to release from liability, indemnify, and hold harmless the school, district, and district personnel against all claims, damages, and costs that may result from my child's use of district technology or the failure of any technology protection measures used by the district. Further, I accept full responsibility for supervision of my child's use of his/her access account if and when such access is not in the school setting. If the device is damaged, due to abuse or neglect, or if the device and/or AC power adaptor is lost, the student must pay a loss/damage fee of up to $200.00.

Name: _____ Date: _____
(Please print)

Signature: _____

Exhibit LAKE TAHOE UNIFIED SCHOOL DISTRICT
version: May 1, 2010 South Lake Tahoe, California
revised: August 5, 2010
revised: October 13, 2015
revised: July 24, 2018
revised: September 10, 2019 (7/23/19: pending board approval)