The purpose of this Employee Acceptable Use of Technology Agreement ("Agreement") is to ensure a safe and appropriate environment for all employees and students.¶
Pursuant, in part, to Board Policy and Administrative Regulation 4040, this Agreement notifies staff about the acceptable ways in which technology may be used at the district, in order to carry out lawful**ACCEPTABLE USE AGREEMENT**
AND RELEASE OF DISTRICT FROM LIABILITY (EMPLOYEES)

The Tahoe Truckee Unified School District authorizes district employees to use ofdistrict technology, including, but not limited to, use of technology in a manner which protects student privacy under state and federal law. The district recognizes and supports advances in technology and provides an array of technology resources for employees to use to enhance the learning environment, facilitate resource sharing, encourage innovation and to promote communication.¶

While these technologies provide a valuable resource to the district, it is important that employees' use of technology be appropriate for district purposes.¶

Pursuant to Board Policy and Administrative Regulation, only employees who submit a signature acknowledging receipt and agreement to the terms of use outlined in this Agreement are authorized to use the district's technology.¶

I. Definitions¶

A. "District technology" includes district owned and maintained or created or authorized electronic technology including, but not limited to, computer hardware and software, electronic devices such as tablet computers, smart phones and cell phones, telephone and data networks (including intranet and Internet access), email systems, electronically stored data, websites, web applications or mobile applications. The definition of district technology expressly includes access to district data networks from devices owned by a User or the district, whether on or off district property.¶

B. "System Administrator" includes the Superintendent Chief Learning Officer or designee, and staff employed by the district and persons employed by district departments whose responsibilities include district technology administration. System Administrators perform functions including, but not limited to, installing hardware and software, managing a computer or network, and keeping district technology operational.¶

C. "User" means someone who does not have System Administrator responsibilities for district technology, but has access to district technology.¶

D. "User Account" means the combination of a User number, User name, and/or User ID and a password that allows an individual User access to district technology.¶

II. District Rights and Responsibilities¶

~~It is the policy of the district to maintain an environment that promotes ethical and responsible conduct in all online network activities by employees. Employees shall not have an expectation of privacy when using district technology or using personal technology on the district's network. It shall be a violation of this policy for any employee to engage in any activity that does not conform to the established purpose, and general rules and policies of the network. The district retains the following rights and recognizes the following obligations:¶~~

~~To monitor employee use of technology to ensure public resources are appropriately used and to ensure that the district's policies and regulations regarding harassment and nondiscrimination, as well as other applicable policies and regulations, are being followed. The district can and does monitor~~as defined in Board Policy 4040 - Employee Use of Technology. The use of district technology is a privilege permitted at the district's discretion and is subject to the conditions and restrictions set forth in applicable board policies, administrative regulations, and this Acceptable Use Agreement. The district reserves the right to suspend access at any time, without notice, for any reason.

The district expects all employees to use technology responsibly in order to avoid potential problems and liability. The district may place reasonable restrictions on the sites, material, and/or information that employees may access through the system. However, the district shall not prevent or restrict access to an employee's mobile or other communications device(s) if there is a need to seek emergency assistance, assess the safety of a situation, or communicate with a person to confirm the person's safety.

The district makes no guarantee that the functions or services provided by or through the district will be without defect. In addition, the district is not responsible for financial obligations arising from unauthorized use, or misuse, of the system.

Each employee who is authorized to use district technology shall sign this Agreement, which indicates that the employee has read and understands this Agreement and Board Policy 4040 - Employee Use of Technology.

Employee Obligations and Responsibilities

A. Employees are expected to use district technology safely, responsibly, and¶

district technology access and activity, including but not limited to, websites visited, content viewed, information posted, applications run, content created and stored, and email sent and received. This monitoring includes User access to private online accounts through district technology. The district reserves the right to access and view any material accessed or stored on district technology or any material used in conjunction with its district technology even if that material is stored on a device that is not owned by the district. Electronically generated content produced by district employees may also be subject to the California Public Records Act, and may be subject to public disclosure.¶

B. To log network use and to monitor and maintain storage space utilization by Users. The district does not assume responsibility or liability for files deleted. Should a User's files be deleted by a System Administrator, the district shall not be liable for the deletion. Users are encouraged to back up important documents via an external drive or device.¶

C. To remove a User account on the network or temporarily revoke or suspend access.¶

D. To provide guidelines and make reasonable efforts to train employees in acceptable use and policies governing online communications.¶

E. To provide internal and external controls as appropriate and feasible. Such controls shall include the right to determine who will have access to district-owned equipment and, specifically, to exclude those who do not abide by the district's terms of use or other policies governing the use of school facilities, equipment, and materials. The district reserves the right to restrict online destinations through software or other means.¶

F. User files and information on district technology may be subject to search by law enforcement agencies for investigations if such files contain information which may be used as evidence in a court of law.¶

III. Terms of Use¶

Activities deemed to be appropriate uses of district technology include the following:¶

A. Instructional Use:¶

1. Use in classroom instruction.¶

2. Development of instructional materials.¶

3. Research connected to academic and instructional concerns and interests.¶

4. Communication with colleagues, students, and professional organizations and institutions if such communications are related to the business of the district.¶

B. Administrative Use:¶

1. District administrative and business communications and transactions.¶

2. Communication with colleagues, students and professional organizations and institutions if such communications are related to the business of the district.¶

3. Research tied to district concerns and interests.¶

C. Incidental Personal Use: The district's technology, including Internet access, are to be used primarily for educationalwork-related purposes and district business. Staff may use the district's Internet access subject to the following limitations:¶

1. Incidental personal use is limited to off-duty time except in cases of emergency.¶

2. Incidental use of district technology by Employees does not extend to family members or other acquaintances who are not employed by the district.¶

3. Incidental use must not result in direct costs to the district.¶

4. Incidental use must not interfere with the normal performance of an employee's work duties or student learning.¶

5. Incidental use must not violate this Agreement.¶

Inappropriate use of district technology includes, but is not limited to, the following:¶

A. Any use of the district's technological resources for illegal and/or unauthorized purpose is prohibited.¶

B. Using district technology to access or view pornography.¶

C. Disclosing any student's personally identifiable information to any outside parties without consent or legal authority to do so. Federal and California law prohibit the district's employees from disclosing a student's personally identifiable information using district technology, personal technology or by any other means without written parental consent. (20 USC 1232g; Education Code 49076, subd. (a).)¶

If a district employee requires a student to use technology in connection with a classroom assignment or extracurricular activity, please be advised that a student's personally identifiable information may be disclosed. district employees are prohibited from entering into an agreement with any third-party provider of technology to provide digital educational software that allows the third-party provider to access, store, or use pupil records without the written permission of the Superintendent Chief Learning Officer or designee.¶

"Personally identifiable information" includes, but is not limitedin accordance with the accompanying board policy and applicable copyright laws. Any incidental personal use of district technology shall not interfere with district business and operations, the work and productivity of any district employee, or the safety and security of district technology. The district is not responsible for any loss or damage incurred by an employee as a result of the employee's personal use of district technology.

The employee in whose name district technology is issued is responsible for its proper use at all times. Employees shall not share their assigned online services account information, passwords, or other information used for identification and authorization purposes, and shall use the system only under the account to which they have been assigned.

Employees shall not gain unauthorized access to, the following:¶

1. Student's name;¶

2. Name of the student's parent or other family members;¶

3. The address of the student or student's family;¶

4. A personal identifier such as the student's social security number, student number, or biometric record;¶

5. Indirect identifiers such as the student's date of birth, place of birth, and mother's maiden name;¶

Other information that alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances to identify the student with reasonable certainty; or**files or equipment of others, access electronic resources by using another person's name or electronic identification, or send anonymous electronic communications. Furthermore, employees shall not attempt to access any data, documents, emails, or programs in the district's system for which they do not have authorization.**

6. **Employees are prohibited from using district technology for improper purposes, including**Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates. (Education Code 49061; 34 CFR 99.3)¶

"Technology" includes**, but is not limited to,** Internet sites, web applications and mobile applications which allow a user or users to share information. Examples of such technology include, but are not limited to, cell phone text messaging, email, iPhone's iMessage, Facebook, Facebook Messenger, Twitter, Instagram, Pinterest, YouTube, LinkedIn, Flickr, Tumblr, Vine, Google Plus +, Google Chat, Skype, online chat rooms, Snapchat, WhatsApp, Weebly, Wix and Prezi.¶

D. Using district technology to gain or attempt to gain unauthorized access to any computer systems, installing remote access software without prior approval, or gaining or attempting to gain unauthorized access to district technology is prohibited.¶

E. Connecting unauthorized equipment to district technology, including the unauthorized installation of any software (including shareware and freeware), is prohibited.¶

Unauthorized attempts to circumvent data protection schemes or uncover security loopholes within or outside of district technology are prohibited. This includes creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secure data.¶

F. Knowingly or carelessly performing an act that will interfere with or disrupt the normal operation of computers, terminals, peripherals, or networks, whether within or outside of district technology (e.g., deleting programs or changing icon names) is prohibited.¶

G. Knowingly or carelessly accessing, transmitting, downloading, tampering, vandalizing, running or installing on any district technology, or giving to another User, a program or file intended to damage or to place excessive load on a computer system or network, files or data is prohibited. This includes, but is not limited to, programs known as computer viruses, Trojan Horses, worms, or any type of pyramid schemes. Deliberate attempts to degrade or disrupt system performance of the network or any other computer system or network on the Internet by spreading computer viruses is considered criminal activity under state and federal law.¶

H. Violating terms of applicable software licensing agreements or copyright laws on district technology is prohibited. Downloading, copying, otherwise duplicating, and/or

~~distributing copyrighted materials without the specific written permission of the copyright owner is prohibited, except that duplication and/or distribution of materials for educational purposes is permitted when such duplication and/or distribution would fall within the Fair Use Doctrine of the United States Copyright Law. Employees should seek written permission from the Superintendent Chief Learning Officer or designee prior to duplicating and/or distributing copyrighted materials.¶~~

~~I. Using district technological resources for commercial activity or for-profit purposes, such as creating products or services for sale, or advertising/promoting non-district sites, commercial efforts and/or events, soliciting votes, or political lobbying is prohibited.¶~~

~~J. Inappropriate mass mailing via district technology is prohibited. This includes multiple mailings to newsgroups, mailing lists, or individuals, (e.g. "spamming," "flooding," or "bombing)". This also includes initiating or propagating electronic chain letters via district technology.¶~~

~~Forging the identity of other Users' names, emails, files, data or machine in an electronic~~use of district technology to:

1. **Access, post, display, create, or otherwise use material that is discriminatory, defamatory, obscene, sexually explicit, harassing, intimidating, threatening, or disruptive**

2. **Disclose or in any way cause to be disclosed confidential or sensitive district, employee, or student information without prior authorization from a supervisor, including sharing confidential information or personally identifiable information with an open artificial intelligence system**

3. **Engage in personal commercial or other for-profit activities without permission of the Superintendent or designee**

4. **Engage in unlawful use of district technology for political lobbying**

5. **Infringe on copyright, license, trademark, patent, or other intellectual property rights**

6. **Intentionally disrupt or harm district technology or other district operations (such as destroying district equipment, placing a virus on district computers, adding or removing a computer program without permission, changing settings on shared computers)**

7. **Install unauthorized software**

8. **Engage in or promote unethical practices or violate any law or board policy, administrative regulation, or district practice**

Privacy

Since the use of district technology is intended for use in conducting district business, no employee should have any expectation of privacy in any use of district technology.

The district reserves the right to monitor and record all use of district technology, including, but not limited to, access to the Internet or social media, Internet searches, browsing history, use of artificial intelligence, communications sent or received from district technology, or other uses within the jurisdiction of the district. Such monitoring/recording may occur at any time without prior notice for any legal purposes including, but not limited to, record retention and distribution and/or investigation of improper, illegal, or prohibited activity. Employees should be aware that, in most instances, their use of district technology (such as web searches or emails) cannot be erased or deleted.

All passwords created for or used on any district technology are the sole property of the district. The creation or use of a password by an employee on district technology does not create a reasonable expectation of privacy.

Personally Owned Devices

If an employee uses a personally owned device to access district technology or conduct district business, the employee shall abide by all applicable board policies, administrative regulations, and this Agreement. Any such use of a personally owned device may subject the contents of the device and any communications sent or received on the device to disclosure pursuant to a lawful subpoena or public records request.

Records

Any electronically stored information generated or received by an employee which constitutes a district or student record shall be classified, retained, and destroyed in accordance with Board Policy/Administrative Regulation 3580 - District Records, Board Policy/Administrative Regulation 5125 - Student Records, or other applicable policies and regulations addressing the retention of district or student records.

Reporting

If an employee becomes aware of any security problem (including, but not limited to, a cyberattack, phishing, or any compromise of the confidentiality of any login or account information), or misuse of district technology, the employee shall immediately report such information to the Superintendent or designee.

Consequences for Violation

Violations of the law, board policy, or this Agreement may result in revocation of an employee's access to district technology and/or discipline, up to and including termination. In addition,

violations of the law, board policy, or this agreement may be reported to law enforcement agencies as appropriate.

Employee Acknowledgment

I have received, read, understand, and agree to abide by this Agreement, Board Policy 4040 - Employee Use of Technology, 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 or when my personal electronic devices use district technology. I further understand that any violation may result in revocation of user privileges, disciplinary action, and/or appropriate legal action.

I hereby release the district, its personnel, and the Governing Board from any and all claims and damages arising from my use of district technology or from the failure of any technology protection measures employed by the district.

Name: _____ Position: _____
(Please print)

School/Work Site: _____

Signature: _____ Date: _____

~~communication via district technology in any way, including, but not limited to, disguising one's identity, impersonating other Users, or sending anonymous email is prohibited. Real names must be used; impersonation and pseudonyms are not allowed. Employees should not give their User name and password to anyone.¶~~

~~K. Knowingly or recklessly posting, transmitting or reproducing materials that are false, slanderous or defamatory about a person or organization, or that otherwise violate existing laws or regulations by using district technology is prohibited.¶~~

~~L. Attempting to monitor or tamper with another User's electronic communications, or reading, copying, changing, or deleting another User's files or software via district technology without the explicit agreement of the owner, is prohibited.¶~~

~~M. Pirating of computer software via district technology is prohibited.¶~~

~~N. Selling, purchasing or encouraging the use of drugs, alcohol or tobacco or other illegal items or substances is prohibited.¶~~

~~O. Intentionally accessing, creating, storing, posting, submitting, displaying, transmitting, using or downloading material, images or language that may be deemed hate mail, profane, lewd, vulgar, rude, inflammatory, disrespectful, abusive, impolite, threatening, harassing, discriminatory, racist, offensive, indecent, obscene, or intimidating is prohibited.¶~~

~~P. Malicious use of any district computer/network to develop programs that harass other Users or infiltrate a computer or computing system and/or damage software components of a computer or computing system, and/or "hacking" internal or external to the district, or attempting to access information protected by privacy laws, is prohibited.¶~~

Q. Use for non-≠academic related bandwidth intensive activities, such as unapproved network gaming or hosting/sharing torrents, is prohibited.¶

R. Hardware and/or software shall not be destroyed, modified, or abused in any way.¶

S. District technology may not be used for downloading entertainment software (or other files not related to the mission and objectives of the district) for transfer to a User's home computer, personal computer, or other device.¶

T. Establishing a network of Internet connections to live communications, including voice and/or video (relay chat), unless specifically authorized by a System Administrator, is prohibited.¶

U. Engaging in personal attacks, including prejudicial or discriminatory attacks such as "cyberbullying" is prohibited.¶

V. Violation of any criminal laws, federal, state or municipal laws or ordinances, as well as board policy is prohibited.¶

W. Any use of district technology to create or disseminate content that is inconsistent with the district's professional standards, is prohibited. The district reserves the right to restrict and remove content that violates the district's professional standards on any district technology. (See Board Policy 4219.21 - Professional Standards.)

X. Creation of websites, blogs or other Internet forums that purport to be or hold themselves out to be district-sponsored without prior written permission from the Superintendent Chief Learning Officer or designee. In deciding whether to grant such approval, the Superintendent Chief Learning Officer or designee may ask for the purpose of the particular use of technology, the proposed content, the person designated to maintain the site, any links which may be contained on the site, and privacy settings.¶

IV. Disclaimer¶

The district cannot be held accountable for the information that is retrieved via the network or district technology. The district will not be responsible for any damages you may suffer, including loss of data resulting from delays, non-≠deliveries, or service interruptions caused by district technology, System Administrators or your own errors or omissions. Use of any information obtained via district technology is at your own risk.¶

The district makes no warranties (expressed or implied) with respect to: (a) the content of any advice or information received by a User, or any costs or charges incurred as a result of seeing or accepting any information; or (b) any costs, liability, or damages caused by the way the User chooses to use his or her access to district technology.¶

V. Security¶

All data must be kept confidential and secure by the User. The fact that the data may be stored electronically does not change the requirement to keep the information confidential and secure. Rather, the type of information or the information itself is the basis for determining whether the data must be kept confidential and secure. If this data is stored in a paper or electronic format, or if the data is copied, printed, or electronically transmitted the data must still be protected as confidential and secured.¶

All software programs, applications, source code, object code, documentation and data shall be guarded and protected.¶

VI. Password Policy¶

Passwords must not be shared with anyone and must be treated as confidential information. Passwords must be changed at least every 180 days. All Users are responsible for managing their use of district Information Technology systems and are accountable for their actions relating to security.¶

VII. Acknowledgement of Receipt & Agreement¶

I acknowledge that I have received, read and understood the Acceptable Use of Technology Agreement, as revised August 2015. I understand that any violations of the Acceptable Use of Technology Agreement may be grounds for disciplinary action, up to and including termination. I understand that a copy of the signed Acceptable Use of Technology Agreement will be placed in my personnel file.¶

_____Signature _____Date¶

_____Print Name