EXHIBIT

STOCKTON UNIFIED SCHOOL DISTRICT
STUDENT ACCEPTABLE USE POLICY
(AUP)

The Stockton Unified School District ("District") recognizes that technology and electronic information services are powerful tools that can enhance learning, improve access to academic resources, and help students become community, college, and career-ready graduates. This Student Acceptable Use Policy ("AUP") aims to ensure appropriate, responsible, ethical, and legal use of technology within the District. The District reserves the right to place reasonable restrictions on the material and network resources accessed.

With the evolution of technology, communication mediums, and information access and transfer methods, the District must continue to define and update a policy that ensures a safe learning environment for students, parents/guardians, and staff, while also safeguarding District technology and data. As such, students must follow the Student Conduct Code, AUP, and applicable laws when using the District's "Technology Services" including, the District's internet, network, database systems, and technology resources.

This AUP must be signed and returned to school in order for your child to use the District's Technology Services for educational purposes.

STUDENT INTERNET ACCESS

A parent/guardian may withdraw their approval at any time regarding their child's access to the District's Technology Services outlined in this AUP. Students are expected to abide by the generally accepted rules of appropriate online behavior and network etiquette. These rules include but are not limited to the following:

1. **Internet Protection Measure**
   The District filters access to its internet and technology to protect staff and students from obscene, inappropriate visual depictions, images, and videos. While the District makes every effort to filter objectionable content and websites, some breaches may occur as new content is regularly added to the internet. However, the internet filter is frequently updated to ensure compliance with federal, state, and local laws, e.g., CIPA, FERPA, and COPPA.

2. **Monitoring and Enforcement**
   The District reserves the right to monitor all technology use on its network. Users have no expectation of privacy when using District resources. Violations of this AUP may result in disciplinary action, including but not limited to suspension or termination of access privileges.

3. **Internet Safety / Cyber Safety (Digital Citizenship)**
   Students will be educated through "digital citizenship" curriculum regarding appropriate online behavior. The topics covered in this "digital citizenship" curriculum include cyberbullying, inappropriate language and material, plagiarism, copyright infringement, personal and District account information protection (including password protection), social networking, digital footprint, and respect for privacy.

4. **Illegal Activities and Vandalism**
   Students will not attempt to gain unauthorized access to the District's technology network or other computer systems (i.e., accessing another person's account or files). In addition, students will not attempt to disrupt computer systems or destroy data through methods including but not limited to uploading, creating, or spreading computer viruses. Students will not use the network for illegal activities such as "hacking" or vandalizing technology resources.

5. Cell Phones and Other Electronic Devices

Cell phones and other electronic devices must not disrupt the educational environment. Use of cell phones and other personal electronic equipment on District campuses is at the discretion of the site administration and classroom teacher and must align with this AUP.

6. Accounts

The District provides all K-12 students with accounts for creating documents, participating in lessons, and logging on to District devices and services. Students are responsible for their accounts. All students will take precautions to protect their accounts from unauthorized users by creating strong passwords and not sharing login information. If students believe their account has been compromised, they must notify school staff immediately.

7. Artificial Intelligence Utilization by Students

Artificial Intelligence ("AI"), defined as is a critical 21st-century resource. Therefore, the District permits students and staff to use AI as an educational tool to enhance student learning, improve efficiency, and support creativity, research, critical thinking, and problem-solving skills. The District is responsible for educating students on ethical ways to utilize AI and has developed the following guidelines for AI use:

1. Responsible Use: Students may only use AI in the classroom and on assignments in ways that align with their teachers' expectations. Students must use AI technologies responsibly and ethically by adhering to all relevant laws, regulations, and District policies. AI tools may only be used for educational purposes, such as research, learning enhancement, and academic projects. Students are prohibited from using AI in any inappropriate manner; prohibited use of AI includes but is not limited to making threats, harassing others, and generating or circulating obscene, harmful, or sexually explicit material.

2. Closed and Open AI: Students in grades TK-12 are permitted to use closed AI, which refers to AI tools integrated into educational software that has been approved by the district for instructional purposes. Students in grade 9 and above are also granted access to open AI, including open-source and generative AI tools such as, but not limited to, ChatGPT and Gemini. The use of open AI is allowed under the direction and guidance of teachers and should be strictly for educational purposes.

3. Respect for Intellectual Property: Students must respect intellectual property rights when utilizing AI technologies and are prohibited from presenting AI-generated work as their original work. *To avoid plagiarism, all students must properly cite AI sources when using AI-generated content.* In addition, any use of AI to create or distribute copyrighted material without permission is strictly prohibited—for example, using AI to impersonate someone else's voice or image.

4. Accuracy: Students should be aware that AI may not always provide accurate, up-to-date information and must check their research and confirm their answers.

5. Fairness and Bias: Students should be aware of potential biases inherent in AI algorithms and models. They will strive to mitigate bias and ensure fairness when using AI technologies. Discriminatory or prejudicial use of AI is strictly prohibited, including but not limited to creating or disseminating biased content.

6. Privacy and Data Security: Students must prioritize the privacy and data security of themselves and others when using AI technologies. These practices include safeguarding personally identifiable information and respecting the privacy settings of any data used. Unauthorized access to AI systems or data or any attempt to breach the District's security systems is prohibited.

7. Reporting: Students should report any concerns, incidents, or violations to appropriate authorities, such as teachers, administrators, or technology support staff. Reporting ensures timely intervention and resolution of issues related to the misuse of AI technologies.

New and emerging technologies that utilize AI will be subject to the general tenets of these AI utilization guidelines.

All students and District personnel must comply with the following:

Applicable Compliance Statutes and Regulations

1. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

2. Family Education Rights and Privacy Act 1974 (FERPA)

3. Copyright Act of 1976

4. Foreign Corrupt Practices Act of 1977

5. Computer Fraud and Abuse Act of 1986

6. Computer Security Act of 1987

7. Children's Internet Protection Act of 2000 (CIPA)

8. Children's Online Privacy Protection Act (COPPA)

9. California Codes:
California Education Code
49073.6 Student records; social media
51006 Computer education and resources
51007 Programs to strengthen technological skills.
60044 Prohibited instructional materials

California Penal Code
313 Harmful matters
502 Computer crimes, remedies
632 Eavesdropping on or recording confidential communications.
653.2 Electronic communication devices, threats to safety

10. SB 1117

11. SB 1584

Related District Board Policies

1. BP 0440: Philosophy, Goals, Objectives, and Comprehensive Plan

2. BP 1113: Community Relations

3. BP 5153: Student Conduct

4. BP 6163.4: Student Use of Technology

And their supporting Administrative Regulations

STUDENTS' RIGHTS

1. **Free Speech**
Students' rights to free speech, as set forth in the Student Conduct Code, also apply to their communication on District's Technology Services.

2. Search and Seizure

Students should expect only limited privacy as their account should not be considered personal and private and may be subject to inspection by authorized District employees.

3. Due Process

The District will cooperate fully with local, state, and federal officials in any investigation of illegal activities conducted through the District's network. If there is a claim that students violated the AUP or Student Conduct Code regarding their use of District's Technology Services, the students will be provided written notice of the suspected violation. They will also have an opportunity to present an explanation before an administrator.

LIMITATIONS OF LIABILITY

The District makes no guarantee that the functions or the services provided by or through the District's Technology Services will be error-free or without defect. The District is not responsible for any damages that students may suffer related to the District's Technology Services, including but not limited to data loss or service interruptions. The District is not responsible for the accuracy or quality of the information obtained through or stored on its Technology Services. The District is not responsible for financial obligations arising from unauthorized use of the District's Technology Services. Because the privacy of system users is not guaranteed, the District is not responsible for the loss of personal information voluntarily disclosed by students in violation of the AUP.

The District may suspend any individual's access to District's Technology Services upon any violation of the AUP.

STUDENT ACCOUNT AGREEMENT

Print Student Name_____ Grade_____

Student ID #_____ DOB._____

I have read the Stockton Unified School District's Acceptable Use Policy. I agree to follow the rules contained in this policy. I understand that if I violate the rules, my account can be terminated, and I may face other disciplinary measures.

Student Signature_____ Date_____

PARENT OR GUARDIAN SECTION

I have read the District's Acceptable Use Policy. I hereby release and agree to hold harmless the District, its personnel, and any of its affiliated institutions from any and all claims or damages of any kind whatsoever arising from my child's use of, or inability to use, the District's internet, network, database systems, or technology resources, including, but not limited to, claims arising from the unauthorized use of the District's internet, network, database systems, or technology resources to solicit, provide, or purchase products or services. I will instruct my child regarding any additional restrictions I may have regarding accessing online materials if such restrictions go above and beyond the restrictions outlined in the District's Acceptable Use Policy. I will emphasize to my child the importance of following the rules for personal safety. I give permission for my child to access Stockton Unified School District's Technology Services and certify that the information on this form is correct. Stockton Unified Technology Services include the District's internet, network, database systems, and technology resources.

Parent/Guardian Signature_____ Date_____

Print Parent/Guardian Name_____ Phone_____

FILE THIS DOCUMENT IN STUDENT'S CUMULATIVE FOLDER