STOCKTON UNIFIED SCHOOL District
Employee 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 employees become community, college, and career-ready graduates. This Employee 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 employee, while also safeguarding District technology and data. As such, employees must follow this AUP, and applicable laws when using the District's "Technology Services" including, but not limited to, the District's internet, network, database systems, and technology resources.

TECHNOLOGY & INTERNET ACCESS

Employees are expected to abide by the generally accepted rules of appropriate online behavior and network etiquette. These include but are not limited to the following:

1. Internet Protection Measure

The District filters access to its internet and technology to protect employee and employees 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)

Employees should adhere to appropriate online behavior, including no cyberbullying, inappropriate language, plagiarism and copyright infringement, sharing of personal and District account information, social networking, inappropriate material, digital footprint, password protection, and respect for privacy.

4. Illegal Activities and Vandalism

Employees will not attempt to gain unauthorized access to the District's Technology Network or any other technology resources. Employees will not use the network for illegal or malicious activities.

Employee 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, Employees will not attempt to disrupt computer systems or destroy data through methods including but not limited to uploading, creating, or spreading computer viruses. Employees will not use the network for illegal activities such as "hacking" or vandalizing technology resources.

5. Accounts

The District provides all Employees with accounts. These accounts are used to create documents, participate in lessons, log onto various devices and other work-related services. Employees are responsible for their accounts and will take all precautions to prevent others from using their accounts by creating strong passwords and will not share their usernames and passwords. If an Employee believes that their account has been compromised, they must notify technology employee or supervisor immediately.

6. Artificial Intelligence (AI) Utilization

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

1. Responsible Use: Use of AI in the workplace environment should align with district goals and objectives. Employees must use AI technologies responsibly and ethically, by adhering to all relevant laws, regulations, and District policies. Employees 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. Respect for Intellectual Property: Employees must respect intellectual property rights when utilizing AI technologies. This includes avoiding plagiarism and properly attributing sources when using AI-generated content. Any use of AI to create or distribute copyrighted material without permission is strictly prohibited. For example, the use of AI to impersonate by using someone else's voice or image.

Employees 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 employees 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.

3. Accuracy: Employees should be aware that AI may not always provide accurate up to date information and they need to check their research and confirm their answers.

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

5. Privacy and Data Security: Employees 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.

6. Reporting: Employees should report any concerns, incidents, or violations to appropriate authorities, such as their supervisor or technology employee. 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 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 Employee 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 6163.4: Employee Use of Technology

4. BP 5153: Employee Conduct

And their supporting Administrative Regulations

Employees RIGHTS

YOUR RIGHTS
Employees should be aware that computer files and communications over electronic networks, which include but are not limited to web conferencing, email, voice mail, are not private. To ensure proper use, the District may monitor employee use of technological resources, including but not limited to email and voicemail systems, at any time without advance notice or consent.

LIMITATION OF LIABILITY
The District makes no guarantee that the functions or the services provided by or through the District system will be error free or without defect. The District will not be responsible for any damage you may suffer, including but not limited to, loss of data or interruptions of service. The District is not responsible for the accuracy or quality of the information obtained through or stored on the system. The District will not be responsible for financial obligations arising through the unauthorized use of the District's technology resources.

"The District will suspend any individual's access to District technology upon any violation of the AUP"

EMPLOYEE ACCOUNT AGREEMENT

Print Employee Name_____ Site/Dept_____

Employee ID #_____

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.

Employee Signature_____ Date_____

\