STAFF TECHNOLOGY ACCEPTABLE USE POLICY

The Santa Paula Unified School District authorizes district employees to use district technology, 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

Employees are expected to use district technology safely, responsibly, and primarily for work-related purposes and in 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 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.

Legal Compliance

Employees must comply with all federal, state, and local laws governing the use of technology. These include, but are not limited to, the Family Educational Rights and Privacy Act (FERPA), the Children's Internet Protection Act (CIPA), the Children's Online Privacy Protection Act (COPPA), the California Consumer Privacy Act (CCPA), the California Electronic Communications Privacy Act (CalECPA), and the California Student Online Personal Information Protection Act (SOPIPA). District employees are responsible for understanding and adhering to these regulations when handling student and staff data. All district digital communications, including email and electronic records, may be subject to public records requests under the California Public Records Act (PRA). Employees must protect the confidentiality of student and staff information and ensure that all technology use aligns with district policies, legal requirements, and ethical best practices. Pursuant to California legislation and Federal E-Rate regulations, SPUSD employs appropriate filtering technology to limit Internet access in an effort to prevent online access to materials that are obscene, contain child pornography, or are harmful to minors. These filtering measures comply with CIPA and other applicable regulations to ensure a safe online environment for students and staff. Any attempts to bypass district filtering measures are strictly prohibited.

Network and Hardware Usage

Employees are expected to use district-owned devices, networks, and related technology resources responsibly and for professional purposes. The following guidelines must be followed:

1. District-provided computers, tablets, projectors, and other hardware must be used for work-related tasks and should not be altered or modified without authorization from the Technology Services Department.
2. Employees must not install or use unauthorized software, applications, or external hardware that could compromise district security.
3. Employees are responsible for reporting lost, stolen or damaged equipment immediately to their supervisor and the Technology Services Department.

4. Employees must log out of district systems when devices are left unattended to prevent unauthorized access to sensitive information.
5. Attempting to bypass security controls, including firewalls, filters, or monitoring tools using VPNs or proxy services.

Unacceptable Behavior

Employees must conduct themselves professionally when using district technology. The following behaviors are strictly prohibited:

1. Using technology resources for personal entertainment, such as streaming movies or playing video games, during work hours.
2. Engaging in cyberbullying, harassment, or discrimination against colleagues, students or the public through any digital platform.
3. Using district technology to send, display, or distribute offensive, obscene, or sexually explicit content.
4. Installing or using unauthorized applications, software, or external storage devices on district-owned computers or networks
5. Using district resources for personal financial gain, political campaigning, or commercial activities unrelated to the district's mission.

Streaming Video Use

District staff cannot use retail streaming services (e.g., Netflix, Hulu, Disney+, Amazon Prime, Apple TV) to show movies in class or at school events. While teachers may use copyrighted materials for instructional purposes under Fair Use, this exception does not extend to consumer streaming platforms. These services are licensed for individual use only and expressly prohibit public screenings. Therefore, to show movies or other copyrighted videos during face-to-face instruction, teachers must use legally purchased physical media (such as DVD or Blu-ray) or a K-12 licensed streaming service (such as Swank Motion Pictures/Movie Licensing USA), which requires a separate license for each performance.

Social Media and Digital Communication

Employees should use district-provided email and communication platforms, such as ParentSquare, for all official district communications. Staff members are prohibited from

engaging with students on personal social media accounts. Employees must ensure that any public social media posts do not misrepresent the district or violate SPUSD policies.

Employees who use social networking tools for educational purposes must do so through accounts specifically created for classroom communication. Personal accounts should not be used for student engagement.

Artificial Intelligence (AI) Usage Guidelines

SPUSD recognizes the potential benefits and challenges of AI in education. To ensure ethical and responsible use, employees must adhere to the following guidelines:

1. AI tools should only be used to support instruction and administrative functions in alignment with district goals and with full compliance to Board Policy 6163.5.
2. Employees must comply with FERPA, COPPA, and other privacy laws when using AI tools, and must not share personally identifiable information (PII) with AI systems unless the system is district-approved.
3. AI-generated content should be carefully reviewed for accuracy and bias before use in instruction or decision-making.
4. Transparency in AI use is required. Students, parents, and staff must be informed when AI tools are being utilized in the classroom or for administrative tasks.
5. Employees must avoid using AI tools for high-stakes tasks, such as grading or evaluation, unless explicitly approved by district policy.
6. AI should not be used to access, create or distribute harmful, deceptive, or inappropriate content.

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, and its personnel, 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.

Employee Name (printed): _____

Position: _____

School/Work Site: _____

Signature: _____ Date: _____