Employee Use of Technology

ACCEPTABLE USE AGREEMENT AND RELEASE OF DISTRICT FROM LIABILITY (EMPLOYEES)

The Salinas City Elementary 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.

Definitions

District technology includes, but is not limited to, computer hardware, software, or software as a service provided or paid for by the district, whether accessed on or off site or through district-owned or personally owned equipment or devices, including tablets and laptops; computer servers, wireless access points (routers), and wireless computer networking technology (wi-fi); the Internet; email; applications (apps), including artificial intelligence (AI) apps; telephones, cellular or mobile telephones, smartphones, smart devices, and wearable technology; or any wireless communication device, including radios.

Employee Obligations and Responsibilities

Employees are expected to use district technology safely, responsibly, and primarily for work-related purposes that support the educational mission and operational needs of the District.

Employees shall use district technology in accordance with applicable laws board policy, administrative regulations, cybersecurity procedures, and professional standards. Employees are responsible for safeguarding district technology, protecting confidential information, maintaining the security of their accounts and devices, and exercising appropriate professional judgment when using digital resources, online services, and artificial intelligence (AI) tools. Any use of district technology that compromises the security, integrity, confidentiality, or effective operation of district systems, data, or services is prohibited.

Acceptable Use
Acceptable use of district technology includes, but is not limited to, the following responsibilities and expectations:

1. The employee in whose name district technology is issued is responsible for its proper use at all times.

2. Employees are required to protect and secure their assigned online services account information, passwords, or other information used for identification and authorization purposes, and shall use the district or online system only under the account to which they have been assigned.

3. Employees shall comply with all district cybersecurity procedures, technology standards, and administrative guidance issued by the Superintendent or designee.

4. Employees are expected to exercise reasonable cybersecurity awareness and diligence when using district technology, including safeguarding credentials, recognizing phishing attempts, maintaining secure devices, and promptly reporting suspected security incidents

5. Employees shall take reasonable precautions to secure district technology, including locking devices when unattended and protecting devices from theft, damage, or unauthorized access

6. Employees shall access, use, and share only the district, employee, or student information necessary to perform their assigned duties.

7. Employees using district-approved artificial intelligence tools for district purposes shall exercise appropriate professional judgment and human review to ensure accuracy, appropriateness, and compliance with district policies and applicable laws.

8. Employees shall use district technology in a professional manner consistent with their responsibilities as public employees and representatives of the district.

Unacceptable Use

Employees are prohibited from using district technology for improper purposes, including, but not limited to, 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 personally identifiable (PII) student information without prior authorization from a supervisor, including sharing confidential information or personally identifiable information with any unauthorized third parties, including any artificial intelligence (AI) system. Confidential information includes, but is not limited to, information in a student's education record, such as their grades and information pertaining to an Individualized Education Plan (IEP)

3. Uploading, storing, or transmitting district records using unauthorized personal cloud storage, file-sharing services, or collaboration platforms (i.e., personal Google Drive, Dropbox, iCloud, etc.)

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

5. Engage in unlawful use of district technology or district resources for political campaigning, political advocacy, or unlawful lobbying activities except as permitted by law and board policy

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. Using district communication systems to distribute spam, chain letters, misinformation, or non-business mass communications

8. Recording confidential meetings, classrooms, student interactions, or employee conversations without authorization or legal consent

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

10. Sharing passwords, authentication tokens, multi-factor authentication (MFA) approvals, or allowing another individual to use an employee's account credentials

11. Circumventing cybersecurity safeguards or engaging in behavior that increases cybersecurity risk, including knowingly bypassing security controls, disabling security protections, or repeatedly engaging in unsafe cybersecurity practices after notification or training

12. Downloading confidential student or employee information onto personal laptops, desktops or other portable storage devices without authorization, even if devices are password-protected

13. Use of AI-powered tools (including but not limited to transcription services, virtual assistants, or generative AI platforms) to record, transcribe, summarize, or generate notes from any district meeting without authorization of the Superintendent

14. Install unauthorized software

15. Using online services and/or programs (free or purchased) without ensuring that the District has an agreement with the vendor that accords with the student data privacy provisions of state and federal law, and without ensuring that the parent has provided written permission for the District to upload student data to the online service or program

16. Engage in conduct that violates any law, board policy, administrative regulation, or professional standards applicable to district employees

17. Using artificial intelligence (AI) systems to generate official district communications, evaluations, recommendations, student discipline documentation, or instructional materials, or other work, without appropriate human review

18. Creating, distributing, or using manipulated or AI-generated audio, video, images, or communications that impersonate students, employees, or district officials without authorization

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.

Preferred Communication Methods

To ensure professional and documented communication, the preferred methods for communicating with parents/guardians are District Email, District Telephone, or In-Person meetings. Employees are strongly discouraged from using personal cellular telephones or text messaging for District business.

Care and Maintenance of District Property

Employees are expected to exercise reasonable care and diligence in the handling of District-provided technology. Any loss, theft, or damage must be reported to the Superintendent or designee no later than the next business day. Pursuant to California Labor Code 2802, the District generally bears the cost of repair for equipment damaged during the normal course of work. However, the District reserves the right to seek reimbursement from an employee if damage or loss is determined to be the result of the employee's gross negligence, willful misconduct, or dishonest acts.

Return of District Technology

Employees shall return all district-owned technology, equipment, access devices, records, and materials issued to them upon request of the Superintendent or designee, upon transfer of assignment, or upon separation from employment. Employees shall not delete, alter, destroy, or withhold district data or records prior to returning district technology. Failure to return district property in a timely manner may result in revocation of access privileges, withholding as permitted by law, or other appropriate administrative action.

Personally Owned Devices

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. 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. Personally owned devices used for district business must maintain reasonable security protections, including password protection, current operating system updates, and device locking

features. The district reserves the right to restrict access from devices that do not meet minimum security requirements. 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. Employees are responsible for preserving business-related text messages on personal devices for four (4) years.

Records and Records Retention

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.

Employees should be aware that their use of district technology is subject to automated retention schedules. Email messages will be automatically removed from the user's active account view (Inbox, Sent, etc.) 30 days after receipt or transmission. As transitory communications, Text messages (Google Chat) will be automatically purged from the user's active application 24 hours after transmission. The District shall maintain a master archive of these communications in a centralized system for four (4) years for legal and audit purposes.

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 Acknowledgement

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: _____

State	Description
Gov. Code 11549.3	Cybersecurity
Gov. Code 3543.1	Rights of employee organizations
Gov. Code 7920.000-7930.170	California Public Records Act
Labor Code 1139	Emergency assistance
Labor Code 2802	Limited employee damage liability
Pen. Code 502	Computer crimes; remedies
Pen. Code 632	Eavesdropping on or recording confidential communications
Veh. Code 23123	Wireless telephones in vehicles
Veh. Code 23123.5	Mobile communication devices; text messaging while driving
Veh. Code 23125	Wireless telephones in school buses
5 CCR 16020-16030	Destruction of Records
Code of Civil Procedure 2023.010	Discovery Sanctions
City of San Jose v. Superior Court	Records Retention

Federal	Description
20 USC 7122	Student Support and Academic Enrichment Grants
20 USC 7131	Internet Safety
47 CFR 54.520 protection measures; E-rate discounts	Internet safety policy and technology