PACIFICA
SCHOOL DISTRICT

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

The Pacifica School District (PSD) authorizes employees to use district technology and district-issued devices as defined in Board Policy 4040: Employee Use of Technology and its exhibits. The use of district technology is a privilege, not a right, and may be revoked at any time without notice. Employees are expected to use district technology and devices responsibly, ethically, and primarily for work-related purposes in accordance with applicable laws and district policies.

The district expects all employees to use technology responsibly in order to avoid potential problems and liability. PSD may place reasonable restrictions on the sites, material, and information employees may access through the system. However, PSD shall not prevent or restrict access to an employee's mobile or other communications device 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 PSD systems will be without defect. PSD is not responsible for financial obligations arising from unauthorized use or misuse of the system.

Employee 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

Unacceptable Uses

Employees are prohibited from using district technology for improper or unlawful purposes, including but not limited 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, or changing settings on shared computers)
7. Install unauthorized software
8. Engage in or promote unethical practices or violate any law, board policy, administrative regulation, or district practice
9. Engage in cyberbullying, impersonation, or anonymous messaging
10. Bypass security systems or attempt to override district technology protections
11. Use district technology or devices for non-district entertainment, including streaming media or gaming

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. Sensitive district data must not be stored on personal devices without authorization. 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.

Data Security and Confidentiality

Employees are responsible for safeguarding all sensitive or confidential data, including but not limited to student records (FERPA), personnel files, financial records, and health data (HIPAA). District-issued devices must not be used to store confidential information on unsecured local drives.

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.

Device Loan Terms

Employees are responsible for the proper care and secure use of all district-issued devices. Any damage, loss, or theft must be reported immediately to the IT Department and the employee's supervisor. Employees may be held financially liable for damage to or loss of district property resulting from negligence. Devices must be kept free of unauthorized modifications, such as stickers or personal decorations, and employees are expected to maintain devices in a clean condition, including screens, keyboards, and casings, using safe, non-damaging methods. All devices and accessories must be returned upon request or at the end of the loan period.

District-issued devices are provided for professional use only, with minimal personal use allowed in accordance with district policy. Devices may not be shared with or used by others. Employees must exercise care when using devices, including keeping food and drink away and ensuring clean hands during use. Unauthorized stickers, physical modifications, or installations are prohibited. Only district-approved software, accounts, and credentials may be used on district-issued devices. All internet and account activity conducted on district devices is subject to monitoring by PSD. Prohibited uses include illegal activity, personal business or commercial ventures, bypassing security settings, or using the device for non-district entertainment or streaming. Employees must

follow all district policies for data protection and may not store confidential information on unsecured local drives.

All district-issued devices must be returned in good working condition, along with all assigned accessories, either to the front desk of the employee's school site or to the District Office front desk. Devices must be cleaned and free of debris or markings before return. Returned devices should be in the same condition as when issued, allowing for reasonable wear and tear. Failure to return a device may result in a delayed final paycheck or other consequences.

Technology Use Beyond the Classroom

District technology may be accessed remotely for work-related or instructional purposes. All district policies, including this Acceptable Use Agreement, apply regardless of the user's location or whether district-owned or personally owned devices are used. Employees are responsible for ensuring safe and responsible use of district systems both on and off site.

Cloud Services and Third-Party Applications

Employees may only use district-approved cloud services (e.g., Google Workspace, Zoom). Uploading sensitive information to unapproved platforms is prohibited.

Incident 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), misuse of district technology, or other related issue, the employee shall immediately report such information to the Superintendent, designee, IT department, or supervisor. Employees must promptly report lost or stolen devices, suspected data breaches or unauthorized access, suspicious digital activity or phishing attempts, and any violations of this Agreement.

Copyright and Intellectual Property

Employees must comply with all applicable copyright laws and respect the intellectual property of others when using district technology. Copying, sharing, distributing, downloading, posting, or installing copyrighted material without proper authorization or licensing is prohibited, and all digital content, including music, videos, images, software, and text, should be assumed copyrighted unless explicitly stated otherwise. Employees may not install or use software from outside sources on district devices without written approval from the Information Technology Department. Violations of copyright law may result in personal liability, disciplinary action, and the district seeking reimbursement for any damages caused by unauthorized use.

Social Media Use

Employees are expected to use social media responsibly, in accordance with district policies, professional standards, and applicable laws. Staff must maintain appropriate boundaries with students, ensure that personal and professional online presences remain separate, and uphold the integrity and reputation of Pacifica School District at all times. Employees may not use personal accounts for school-related communication with students or parents, and they must not initiate or accept friends or follow requests from current students on personal accounts. All communication with students must take place only through district-approved platforms.

Employees must also protect confidentiality by refraining from posting or sharing any student-related, personnel-related, or sensitive district information online. Because staff may be perceived as representatives of the district even on personal accounts, they must avoid posting content that could be viewed as inappropriate, inflammatory, discriminatory, or inconsistent with district policies. Personal social media use during instructional or duty time is prohibited unless explicitly authorized for instructional or communication purposes. The use of district logos, school names, mascots, or branding on personal accounts requires written approval from the Superintendent or designee. Finally, employees are responsible for reporting any inappropriate, harmful, or concerning online content involving students or staff to their supervisor or district administrator immediately.

Compliance and Legal References

This Agreement is supported by federal and state laws, including but not limited to:

- CIPA, FERPA, HIPAA, Copyright Act, Computer Fraud and Abuse Act
- California Government Code, Penal Code, and applicable Education Code provisions
- PSD Board Policies 4040, 5125, 6163.4, and related regulations

Consequences for Violations

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. Employees may also be held financially liable for damaged or unreturned equipment.

Employee Acknowledgment

By signing below, I acknowledge that I have received, read, understand, and agree to abide by this Agreement, Board Policy 4040 – Employee Use of Technology, and all other applicable district policies, administrative regulations, and laws governing the use of district technology. I accept

responsibility for the safe, lawful, and ethical use of district technology and devices, and I understand that there is no expectation of privacy when using district technology or when personal devices connect to district systems. I agree to return district-issued devices and equipment upon request or separation from the district, and to complete annual training on technology use, cybersecurity, and data protection. I understand that violations may result in the revocation of user privileges, disciplinary action up to and including termination, financial liability for damaged or unreturned equipment, and/or referral to law enforcement as appropriate.

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: _____
School/Work Site: _____

Employee Signature: _____ Date: _____
Supervisor Signature: _____ Date: _____