The Jefferson Elementary School District and the San Joaquin County Office of Education Data Processing Joint Powers Authority, hereinafter referred to as the "district", authorizes district employees to use technology owned or otherwise provided by the district as necessary to fulfill the requirements of their position. 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 policies, administrative regulations, and this Acceptable Use Policy and Computer 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.

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 of the system.

Each employee who is authorized to use district technology shall sign this Acceptable Use Policy and Computer Use Agreement as an indication that they have read and understand the agreement.

Definitions

District technology includes, but is not limited to, computers, the district's computer network including servers and wireless computer networking technology (wi-fi), the Internet, email, software, cloud applications, artificial intelligence (AI) systems, USB drives, wireless access points (routers), tablet computers, smartphones and smart devices, telephones, cellular telephones, wearable technology, any wireless communication device including emergency radios, and/or future technological innovations, whether accessed on or off site or through district-owned or personally owned equipment or devices.

Employee Obligations and Responsibilities

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

Employees shall not use a non-district issued email or online storage account for conducting district business unless the Superintendent or designee authorizes such use. 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. Employees shall use passwords with a minimum of 14 characters on all systems used to conduct district business and operations or the maximum number of characters if the system enforces a shorter limit. Employees shall not use these passwords for systems other than those used to conduct district business and operations. Employees shall use Multi-Factor Authentication (MFA) on all systems that provide a MFA option. Employees shall participate in annual Cybersecurity training offered by the district.

Employees are prohibited from using district technology for improper purposes, including, but not limited to, use of district technology to:

1. Access, post, display, 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.
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, changing settings on shared computers).
7. Install unauthorized software.
8. Engage in or promote unethical practices or violate any law or district policy, administrative regulation, or district practice.
9. Bypass or disable any security software, settings, or configurations.

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, 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, they shall abide by all applicable policies, administrative regulations, and this Acceptable Use Policy and Computer Use 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 other lawful 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 policies 3580 - District Office Records, 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 (such as any compromise of the confidentiality of any login or account information) or misuse of district technology, they shall immediately report such information to the Superintendent or designee.

Consequences for Violation

Violations of the law, district policy, or this Acceptable Use Policy and Computer Use 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, district 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 Acceptable Use Policy and Computer Use Agreement, 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.

Name: _____ Employee ID: _____
(Please print)

Signature: _____ Date: _____