Delano Union School District
Staff Acceptable Use Policy

Purpose and Scope

This policy establishes the standards and expectations for all district employees regarding the use of technology and information resources. It applies to the use of any district-owned or district-provided computers, mobile devices, software, email accounts, networks, and any personal devices used for school business. All technology use shall support the district's educational mission and comply with applicable federal laws (e.g., FERPA, COPPA, SOPIPA) and board policies governing student records, communications, and data security. In particular, staff shall use district resources "primarily for purposes related to their employment" and shall be responsible for their appropriate use. District technology is provided to enhance instruction and operations, and all users shall protect these resources and the information contained in them.

Educational Purpose

District technology resources are intended to enhance teaching, learning, communication, and administrative duties. Employees may use technology, including approved educational applications and artificial intelligence tools, to develop curriculum, analyze student work, communicate with colleagues and families, and support instructional strategies. All use of technology shall align with the district's curricular goals and vision, furthering student learning and staff professional growth. Authorized technology use must never compromise educational standards. Staff are responsible for ensuring that any content generated or shared via technology is pedagogically appropriate and age-appropriate for K–8 students.

Student Data (Staff Responsibilities)

Staff are custodians of student records and shall handle all student data with the highest confidentiality. Consistent with the Family Educational Rights and Privacy Act (FERPA) and Board Policy 5125, only authorized personnel with a legitimate educational interest may access or disclose student educational records. The Superintendent or designee shall ensure that staff receive training in data privacy and record-keeping procedures. Staff must not share personally identifiable student information (such as grades, health or special education records, test results, or behavioral data) with unauthorized individuals or third parties, except as permitted by law. Any violation of student privacy or testing confidentiality will result in discipline in accordance with law and district regulations. Employees shall immediately report any actual or suspected breaches of student data privacy to the appropriate administrator.

No Employee Privacy Rights

Employees have no privacy rights whatsoever in their personal or work-related use of District technology, or to any communications or other information contained or that may pass through District technology. With or without cause and with or without notice to the employee, the

County Office retains the right to remotely monitor, physically inspect, or examine District computers, electronic devices, network, or other District technology, and any communication or information stored on or passing through District technology, including but not limited to software, data and image files, internet use, emails, text messages, and voicemail.

All email sent and received via the District email system, including email of a personal nature, will be captured and retained in a central location for a period of time determined by the District to be appropriate. Deletion of email from computers and electronic devices will not delete captured and retained email. The email that is captured and retained in a central location is the District's official record of the email, no matter where other copies of that email may be found.

District technology will be inspected for software and/or virus-like programming, including commercial software applications that harvest, collect, or compromise data or information resources. Any computer or electronic device containing those elements may be disconnected, blocked, or otherwise isolated at any time and without notice in order to protect District technology. This includes personal computers and/or electronic devices that an employee may connect, with or without proper authorization, to District technology. Due to the commonplace presence of such software and applications on personal computers and/or devices, their connection to District technology without prior authorization is discouraged."

At no time, including when an employee leaves employment with the District, shall the employee delete District electronic records unless expressly authorized to take such action. Management shall be given access to and the authority to dispose of any and all District electronic records, including the employee's computer files, email, voicemail, text messages and any other electronic information stored on District devices

Acceptable Use of Technology

Employees shall use district technology resources responsibly, efficiently, and primarily for purposes related to their job duties. All district computer systems, networks, and data are intended for educational and operational activities. Personal use of district technology must be minimal and shall not interfere with professional responsibilities. Staff shall abide by all relevant board policies and administrative regulations when using digital resources, including policies on intellectual property and confidentiality. Any use of district technology (including email, internet access, and software applications) must be appropriate, respectful, and consistent with the district's values and legal requirements.

Student Data Privacy Commitment

The district is committed to protecting student privacy and complying with all applicable laws governing student information. Staff shall adhere to FERPA and the Children's Online Privacy Protection Act (COPPA), as well as California's Student Online Personal Information Protection Act (SOPIPA). Any third-party educational technology that handles student data must be covered by a signed contract meeting California Education Code requirements (including Ed. Code 49073.1) to ensure appropriate data security and privacy protections. Vendors are prohibited from selling student information or using it for targeted advertising. For students under age 13, staff must ensure that any online service obtains the required parental consent

for data collection and account creation. Staff shall not provide student data to unauthorized persons or entities and shall only share student information under circumstances permitted by law or district policy.

Prohibited Activities and Misuse

District technology resources may not be used to facilitate activities that violate law or district policy. Examples of prohibited uses include, but are not limited to:

- Accessing, posting, or distributing illegal, obscene, threatening, or violent content via district devices or networks. This includes pornographic material, hate speech, and content that is “harmful matter” under California Penal Code 313 (which appeals to prurient interest or depicts sexual conduct offensively to minors).

- Sharing confidential student or staff information without proper authorization or for non-educational purposes.

- Using district technology to undermine the integrity of assessments or to engage in academic dishonesty (for example, altering test answers, sharing secure testing materials, or giving improper assistance during tests).

- Engaging in harassment, bullying, or any form of abuse or discrimination of others using district technology.

- Attempting to gain unauthorized access to restricted systems, networks, or data (hacking), or to bypass district security filters or monitoring tools.

- Installing or using non-district-approved software, applications, or hardware that could compromise system security or stability.

- Using district technology for personal financial gain, commercial enterprises, lobbying, or any other activity not related to the district’s mission.

- Downloading or copying copyrighted material (including software, music, or video) without permission; see the **Copyright and Intellectual Property** section for details.

Any activity that violates local, state, or federal law is strictly forbidden. Inappropriate use of district technology may result in cancellation of network privileges, disciplinary action, or legal action under applicable laws and board policies.

Employee Use of Artificial Intelligence Applications

Artificial Intelligence can be defined as “automation based on associations.” When computers automate reasoning based on associations, (in data or associations deduced from expert knowledge), two shifts fundamental to artificial intelligence occur and take computing beyond conventional educational technology as follows: (1) from merely capturing data to detecting patterns in data; and (2) from providing mere access to instructional resources to automating decisions about instruction and other educational processes. Detecting patterns and automating decisions are leaps above the level of responsibilities that have been typically delegated to a computer system. Note however, that the process of developing an artificial intelligence system may lead to bias in how patterns are detected and unfairness in how decisions are automated. – (U.S. Department of Education, Office of Educational Technology, Artificial Intelligence and Future of Teaching and Learning: Insights and Recommendations, Washington, DC, 2023.)

Artificial Intelligence may assist staff with drafting emails, documents, data analysis, streaming tasks and idea generation. Artificial Intelligence is incorporated into educational software that staff may use when developing lesson plans or instructional presentations. Use of artificial intelligence for these purposes is encouraged.

When using such technology staff are required to be cognizant of, and sensitive to, the potential for errors in, and misperceptions created by, artificially generated content and also inappropriate and wrong output that may automatically result from algorithmic bias.

Staff are reminded that academic honesty and personal integrity are required at all times. Any use of artificial intelligence which demonstrates a lack of academic honesty or personal integrity is prohibited.

Before allowing students to use a specific artificial intelligence platform, teachers will have the system vetted and approved by the District Technology Department and Program Administrator.

Any use of artificial intelligence applications in the classroom or on class assignments must align with the teachers’ instructions and use expectations. Teachers will clarify whether students are prohibited from using artificial intelligence technology in an assignment. Teachers will guide and monitor student use of artificial intelligence technology.

Bias and Discrimination

District technology must not be used to promote bias, discrimination, or harassment. Employees shall not create, access, or distribute any content that demeans or targets individuals or groups on the basis of race, color, national origin, sex, gender identity, sexual orientation, religion, disability, or any other protected characteristic. Board policy explicitly prohibits posting content on official district sites that is obscene, libelous, or that incites unlawful acts. The district’s nondiscrimination and anti-harassment policies apply to all digital interactions: staff must treat all students, parents, colleagues, and community members with respect and refrain from using

technology to propagate stereotypes or to harass others. Any use of technology that violates the district's equity and inclusion obligations will result in corrective action.

Email and Communication Guidelines

Employees shall use district-approved email accounts and communication channels for all official school business. Communications should be professional, courteous, and focused on district goals. Staff are required to use clear and grammatically correct language, and should follow any district style or branding guidelines in their messages. All official communications are considered public records under the California Public Records Act, and employees shall have no expectation of privacy when using district equipment or accounts. Employees should avoid using personal email or social media accounts for substantive district business; if such use occurs, they must be prepared to produce those communications when requested by the district. Confidential or sensitive information (such as student grades, health data, or personal staff information) shall never be transmitted through unsecured or unauthorized channels.

Social Media and Public Communication

When communicating on social media or other public platforms, staff must comply with Board Policy 1114 and district guidelines. Official district social media accounts and websites are managed by designated personnel and shall be used only for approved district purposes. All public posts and content must serve an official purpose (aligned with district vision and educational objectives) and meet district standards for appropriateness. Privacy of students and staff must be safeguarded: employees shall not post private directory information (such as home addresses or phone numbers) or confidential data on public sites. Student photos or names may only be published if parents/guardians have granted permission and any directory opt-outs have been observed. Personal social media accounts should clearly indicate they are personal, and staff shall not use them to discuss confidential district matters or to make harassing or derogatory comments about others. In all public communications, employees shall be courteous, professional, and factually accurate.

Use of District-Approved Apps and Platforms

Staff shall use only district-approved educational applications and online platforms when working with students or handling student data. The district maintains a list of approved vendors that meet privacy, security, and instructional standards. Any third-party provider handling student information must have a formal contract that complies with California law (such as Ed. Code 49073.1) and SOPIPA requirements. Employees shall not introduce or subscribe to new software, websites, or digital services involving student data without prior approval from the district technology department. If staff wish to use a new tool, they must obtain confirmation that the vendor has been vetted and approved by the district.

Unvetted Educational Content

Employees shall critically evaluate all online resources and content before sharing them with students. Only materials that are age-appropriate, accurate, and aligned with the district curriculum shall be used. District and school websites and social media shall not include content

that is obscene or otherwise inappropriate. Staff should verify the credibility of websites, apps, and digital media, and should not rely on or distribute unverified or biased information. Any outside video, game, or article used in instruction should have been reviewed and approved to ensure it meets educational standards and is suitable for K–8 learners.

Ownership

District technology acquired with District funding is provided to meet mission accomplishment needs and does not belong to employees. Use of District technology is a privilege which may be revoked or restricted at any time without prior notice to the employee.

All District computers and other electronic devices are to be registered to the District and not to an employee. All software on District computers and other electronic devices is to be registered to the District and not to an employee, except as otherwise provided in District policy.

No employee shall remove a District computer or other electronic device from District property without prior express authorization of the employee's supervisor.

Password Protections Required

To help protect against unauthorized use of and/or access to District technology and electronic records, all District computers and other electronic devices that can be password protected must be password protected, even if a computer or electronic device is assigned to a single employee for his or her sole use.

All personal computers and other electronic devices connected to District technology, including the email system, or which otherwise contain District electronic records or can be used to access to those records, shall have user passwords installed and utilized to preclude unauthorized access to and/or use of the personal computer or device and/or its connection to District technology. Whenever possible, individual programs, applications, and/or connections on personal computers and electronic devices shall each be password protected, requiring manual entry of a password before the computer or device can connect to any District technology, including email, or to any District electronic records. District passwords should be different from personal passwords.

Any screensaver that can be password protected must be password protected in addition to any network login requirement. Whether or not password protection is technologically feasible, the employee who owns a computer or electronic device that can be connected to District technology, or that contains County Office electronic records, shall be responsible for physically protecting it against unauthorized use.

The Superintendent/designee may authorize and require installation of special software on District devices to enable remote shutdown to prevent unauthorized disclosure of District records should the device be lost or stolen. The Superintendent/designee may authorize

installation of special software on personal devices that may contain County Office records, or have access to County Office records, to enable remote shutdown should the device be lost or stolen. Employees shall promptly report to their supervisor when County Office EIR technology or any personal computer or device containing County Office records or connections is lost or stolen.

Device Management and Care

District-issued devices (such as laptops, tablets, and smartphones) are district property and shall be properly maintained. Staff shall use these devices for work-related purposes and keep them clean, charged, and in good working order. Users must not remove or disable security features, install unauthorized software, or alter device configurations without permission from the technology department. If a district device is lost, stolen, or malfunctions, the employee must report the issue immediately so that data can be secured and the device repaired or replaced. Staff are responsible for backing up any important work files according to district procedures.

Copyright and Intellectual Property

Employees shall respect the intellectual property rights of content creators. All use of copyrighted text, images, audio, video, software, and other media must comply with copyright law and Board Policy 6162.6 (Use of Copyrighted Materials). Staff may use copyrighted materials only with permission from the copyright holder or under permissible exceptions (such as fair use for education). Copying or distributing copyrighted software, music, or videos without a valid license is prohibited. Any original work produced by employees in the course of their duties (such as curricula, presentations, or publications) becomes part of the district's materials and must follow the district's guidelines for publication and use.

Monitoring, Enforcement and Reporting

The district reserves the right to monitor all use of its technology resources to ensure compliance with this policy. Employees shall have no expectation of privacy when using district devices, networks, or accounts. The Superintendent or designee may review email, files, and internet usage at any time, without advance notice, in accordance with law. Staff are required to promptly report any security incidents, breaches, or misuse of technology to the appropriate administrator. The district will investigate any alleged violations and may involve law enforcement if illegal activities are suspected.

Digital Citizenship

Staff are expected to model positive digital citizenship. This includes demonstrating respectful communication online, practicing academic honesty, and protecting the privacy and rights of others. Employees should teach and encourage students to use technology safely and ethically, including evaluating online sources for credibility and respecting intellectual property. The district supports professional development in digital literacy and safe online practices so that staff can effectively guide students in responsible technology use.

Informed Consent

Certain uses of student information and media require prior informed consent from parents or guardians. Board policy and state law require that parents be notified and given the opportunity to opt out of the release of directory information and certain school activities. Staff must honor any parental opt-out requests (for example, withholding a student's photo, name, or directory data from public release). No personally identifying information beyond directory data shall be used in school publications, websites, or promotions without explicit parental permission. Teachers and staff must also obtain parent/guardian permission before involving students in any online service or activity that collects personal information or requires accounts.

AI and Age-Appropriate Interaction

Employees may use approved artificial intelligence tools to support instructional planning and student learning, but only in compliance with district guidelines. As Board Policy 4040 notes, any use of AI by staff must respect student privacy (for example, not sharing confidential student records with an AI service) and shall comply with existing laws and policies. All AI-generated content or recommendations should be carefully reviewed by the teacher before use, and must be suitable for K–8 students in content and complexity. Staff should not allow unsupervised interactions between young children and any AI chatbot or online agent. Whenever AI or other advanced technologies are used with students, they must be used in a manner consistent with the district's age-appropriate standards and curricular objectives.

De-identification of Student Records

When student data are used for research, reporting, or any purposes outside direct instruction, all personally identifiable information shall be removed. Student names, ID numbers, and other direct identifiers should be stripped from datasets in compliance with FERPA and district policy. Reports or analyses should use only aggregated or anonymized data unless there is a specific legal exception or parental consent on file. This practice ensures that individual students cannot be identified from any shared or published information, thereby protecting student privacy.

Consequences for Violation

Any violation of this policy may result in disciplinary action up to and including termination of employment, as well as possible civil or criminal liability, consistent with law and collective bargaining agreements. Inappropriate or illegal use of technology will result in the suspension of access privileges and other sanctions under district policy. The district will pursue appropriate penalties if an employee's actions result in harm to students or staff or compromise the security of district systems.

Employee Acknowledgment

All employees shall be required to sign this agreement indicating that they have read, understood, and will comply with this Acceptable Use Policy. The superintendent or designee shall maintain records of these acknowledgments. Employees must also acknowledge any

significant updates to this policy when they occur, as a condition of continued access to district technology resources.

Sources: District policies and procedures (BP 4040, BP 5125, BP 1114, BP 1113, BP 1100, BP 6162, BP 3580) and state/federal laws (FERPA, COPPA, SOPIPA, and relevant Education and Penal Codes) as cited above. These sources guide the obligations and restrictions reflected in this policy.

Name: _____ Position: _____
(Please print)

School/Work Site: _____

Signature: _____ Date: _____