MERCED CITY SCHOOL DISTRICT

EMPLOYEE TECHNOLOGY ACCEPTABLE USE AGREEMENT

The purpose of this Acceptable Use Agreement ("Agreement") is to ensure a safe and appropriate environment for all Employees. This Agreement notifies staff about the acceptable ways in which District Technology may be used. The Merced City School District ("District") recognizes and supports advances in technology and provides an array of technology resources for Employees to use to enhance student learning, facilitate resource sharing, encourage innovation, and to promote communication. While these technologies provide a valuable resource to the District, it is important that Employees' use of technology be appropriate for District purposes.

The use of District Technology is a privilege and not a right. Inappropriate use, including any violation of the law, Board policies, administrative regulations or this Agreement may result in suspension or revocation of the privilege. Pursuant to Board Policy 4040, only Users of District Technology who submit a signature acknowledging receipt and agreement to the terms of use outlined in this Agreement are authorized to use the District's Technology. To remain an eligible User, the use of your account must support and be consistent with the educational objectives of the District.

Terms of Use

Acceptable Use: District Employees are only permitted to use District Technology for purposes which are safe (pose no risk to students, Employees or assets), legal, ethical, do not conflict with their duties or the mission of the District, and are compliant with all other District policies. Usage that meets these requirements is deemed "proper" and "acceptable" unless specifically excluded by this policy or other District policies. The District reserves the right to restrict online destinations through software or other means.

Additionally, the District expressly prohibits:

1. Transmitting communications or messages which promote unethical practices or violate District or School policies, applicable software license agreements, or state and federal laws, including, but not limited to, copyright, trademark or trade secrets law;
2. Using District Technology for commercial gain, including transmission of advertising, promotional materials or other forms of solicitation;
3. Accessing District Technology for the purpose of gaming or engaging in any illegal activity;
4. Using District Technology to gain unauthorized access to any electronic communications system, network or file;
5. Transmission of confidential information to unauthorized recipients;
6. Intentionally or negligently disclosing a User's password or account number to any other person who does not have authorization to view that password or account number;

7. Inappropriate and unprofessional behavior online such as use of threats, intimidation, bullying or "Flaming";

8. Viewing, downloading, or transmission of pornographic material;

9. Using District Technology for the creation or distribution of Chain E-mails, any disruptive, defamatory or offensive messages, offensive comments about race, gender, disabilities, age, sexual orientation, religious beliefs/practices, political beliefs, or material that is in violation of workplace harassment or workplace violence laws or policies;

10. Engaging in unlawful use of District Technology for political lobbying;

11. Significant consumption of District Technology for activities unrelated to District business (such as video, audio or downloading large files) or excessive time spent using District Technology for non-business purposes (*e.g.*, shopping, personal social networking, or sports-related sites);

12. Knowingly or carelessly performing an act that will interfere with or disrupt the normal operation of computers, terminals, peripherals, or networks, whether within or outside of District Technology (*e.g.*, deleting programs or changing icon names) is prohibited;

13. Infringing on copyright, license, trademark, patent, or other intellectual property rights; or

14. Disabling any and all antivirus software running on District Technology or "Hacking" with District Technology.

Accountability: Users are prohibited from anonymous usage of District Technology. In practice, this means Users must sign-on with their uniquely assigned District User ID before accessing/using District Technology. Similarly, "Spoofing" or otherwise modifying or obscuring a User's IP Address, or any other User's IP Address, is prohibited. Circumventing User authentication or security of any host, network, or account is also prohibited. Access to networks other than the District's is made possible through an appropriate provider designated by the Merced County Office of Education ("MCOE") at its sole discretion. District Users must comply with the terms of this Agreement and any policies or requirements governing the use of other networks they access using District Technology.

Personal Use: District Technology is provided solely for the conduct of District business. However, the District realizes and is aware of the large role technology (especially the Internet and e-mail) plays in the daily lives of individuals. In this context, the District acknowledges that a limited amount of personal use of District Technology is acceptable. This use must not interfere with the User's job responsibilities; it cannot involve any activities expressly prohibited by this or any other District policy; and it should be limited to designated break periods and/or the User's lunch break except in the case of safety issues or other emergency.

Disclaimer: The District cannot be held accountable for the information that is retrieved via the network. The District will not be responsible for any damages you may suffer, including loss of data resulting from delays, non-deliveries, or service interruptions caused by the District Systems, System Administrators or your own errors or omissions. Use of any information obtained is at your own risk.

The District and MCOE make no warranties (expressed or implied) with respect to: (a) the content of any advice or information received by a User; (b) any costs or charges incurred as a result of seeing or accepting any information; (c) any costs, liability, or damages caused by the way the User chooses to use his or her access to the network; or (d) injuries or damages resulting from exposure to inappropriate, offensive, harmful or controversial materials, whether User initiated or otherwise.

Security/Password Policy: Security on the District computer system is high priority, especially as the system involves many users. Passwords must not be shared with anyone and must be treated as confidential information. Passwords must be changed as often as required by the District's IT Department. All Users are responsible for managing their use of District Technology and are accountable for their actions relating to security. Allowing the use of your account by another User is also strictly prohibited. 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. Attempts to log-on to the network as a system administrator will result in cancellation of your User privileges. Any User identified as a security risk will be denied access to the network.

Responsibility: Users are responsible for their own use of District Technology and are advised to exercise common sense and follow this Agreement in regard to what constitutes appropriate use of District Technology in the absence of specific guidance.

Network Use: All Users will be assigned a data storage folder on a District network file server to which they are to save all files or other data, as well as a "Google Drive" folder. The District data folder is accessible only to the User and to network administrators. The Google Drive folder may be shared by instructional staff with students to facilitate collaboration and communication between teachers and students. Attempting to access another User's folder is prohibited. Other shared folders to which a User has access may be created with the approval of a System Administrator. All other storage areas on the District network should not be accessed. Attempting to access any file, folder, printer or other resource on the District network to which you have not been given access is prohibited. All rules of professionalism, safety and security regarding use of student and District data apply while accessing District-network information from outside the network (*e.g.,* from home or public venues).

Security Camera Use: Users whose position requires access to security cameras for school grounds or administrative locations will be assigned a security camera account. The account will be configured with access to cameras that are appropriate for the individual position. The District Camera system should be up and running on video walls continually but should not be left up and running on individual computers or mobile devices. The system should only be accessed as needed within the scope of the user's position. The user may only log into the camera system when there is a specific reason or need related to their position that requires access to the camera system. Access to the camera system does not imply an authorization to surveille or monitor the camera system. Only an authorized position may surveille or monitor the camera system as appropriate. Unauthorized surveillance or monitoring of the camera system is not allowed and may be subject to disciplinary action.

Users agree that they are responsible for any passwords provided to them for the use of the camera system and are not to share the password with anyone else. If a user does not have access to the security camera system and feels that it is within their job requirements to have access, they shall write a request to their Site Admin/Director who will contact Human Resources explaining the need for camera access. Users or employees are not to "borrow" or make use of another user's computer to view cameras or stored video from the District Camera system. All requests for access to the camera system or requests for video or photographs shall go through an employee's direct supervisor. All rules of professionalism, safety and security regarding use of District technology apply while accessing the District Camera system.

Electronic Mail: All Users are provided a District e-mail account as well as a District-managed Google account. Users may use their e-mail accounts to send messages to other District Users or any Internet e-mail account holder so long as the content and language of the message or any associated attachment is consistent with all of the provisions of this Agreement. All e-mail communications must be professional in nature and used for official District business and communication. District Users are responsible for managing the contents of their District e-mail accounts. Users will not use their District provided email accounts to register for non-work related services or in non-work related websites including, but not limited to, on-line banking, gym memberships, on-line periodicals, shopping sites (e.g. Amazon, etc), medical web portals, gaming websites, home or auto-loan websites, or non-work related social media accounts. Users will not use District provided email accounts to exchange medical or other personal sensitive information about themselves or anyone in their family. Users will not transmit or store any sensitive personally identifiable information in their email accounts such as social security numbers, credit card information, vehicle identification numbers, loan information, financial accounts or any other personal information which, if obtained by cyber criminals, could be used for extortion.

Email Archiving and Storage: All District e-mail will be archived in a separate archiving system up to a maximum of three years. All users will be able to access only their own District archived email from within the archiving system. E-mail stored on the local District email server will be restricted by size limits. If the amount of information in the accounts exceeds the size limits for the account becomes too large, you may be contacted by the IT Department to delete items until the amount of information is below the limits required for safe operation of the e-mail servers. IT staff may assist Users with the safe off line storage of e-mails and with its deletion from the e-mail server. E-mail will be stored/archived for a minimum of one year after an account is closed due to inactivity.

Internet Websites: District sites, schools or classes may establish websites that present information about the District site, school or class. The school principal or site administrator is responsible for reviewing all materials that appear on the Internet website. The District webmaster will communicate with District IT personnel to maintain and update any District website. All material on a District website must adhere to the District Copyright Policy as well as all other District policies and regulations. Under no circumstances may students be identified by name, or have any personal information published on the Internet either using District Technology or on a District website. The District's IT Department is responsible for maintaining the District website servers and/or services and may assist and train other site administrators and staff on how to safely and effectively upload content in an approved manner.

Revocation of Authorized Possession: The District has sole discretion to determine appropriate use and may deny, revoke, suspend, or close any User account at any time based upon a determination of inappropriate use by any User. The District reserves the right, at any time, for any reason or no reason, to revoke a User's permission to access, use, or possess District Technology.

Restriction of Use: The District reserves the right, at any time, for any reason or no reason, to limit the manner in which a User may use District Technology in addition to the terms and restrictions already contained in this Agreement.

Vandalism and Harassment: Vandalism or harassment, as defined herein, will result in cancellation of network privileges.

Penalties for Improper Use: Any User violating these rules, applicable state and federal laws, or posted classroom and District rules is subject to loss of network privileges, other District disciplinary options, as described in the Collective Bargaining Agreement. In addition, pursuant to California Penal Code section 502, unauthorized Internet access, attempted access, or misuse of any state computing and/or network system may be subject to a report to law enforcement authorities and, if appropriate, criminal prosecution.

Third-Party Technology: Connecting unauthorized equipment to the District Technology, including the unauthorized installation of any software (including shareware and freeware), is prohibited. Only IT personnel or someone authorized by the District IT Department may install, troubleshoot, or configure software or hardware.

Personally Owned Devices: If an Employee uses a personally owned device to access District Technology or conduct District business, he/she 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.

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, he/she shall immediately report such information to the Superintendent or designee. If you identify or perceive a security problem on the network, notify the District's IT Department; do not demonstrate the problem to others.

Consequences for Violation: Violations of the law, Board policy, administrative regulations, or this Agreement may result in revocation of an Employee's access to District Technology and/or restriction of his/her use of District Technology and/or discipline as described in Article XIII of the Certificated Collective Bargaining Agreement. In addition, violations of the law, Board policy, administrative

regulations, or this Agreement may be reported to law enforcement or other agencies as deemed appropriate.

Network Etiquette

All Users shall abide the generally accepted rules of network etiquette. These include, but are not limited to, the following:

- Be polite. The content of all communications shall be professional in nature and befitting a K-8 educational institution.
- Use appropriate language. Do not swear, use vulgarities, or use any other inappropriate language.
- Do not use the network such that you disrupt the use of the network by other Users.
- Do not plagiarize work, material or ideas from others who have posted it on the Internet.
- Do not reveal personal information regarding students or colleagues, including telephone numbers, home addresses or any other confidential information.

Enforcement

Record of Activity: User activity with District Technology may be logged by System Administrators. Usage may be monitored or researched in the event of suspected improper District Technology usage or policy violations.

Blocked or Restricted Access: The District has sole discretion to determine whether a site, service or protocol will be blocked to Users. User access to specific Internet Resources, or categories of Internet Resources, deemed inappropriate or non-compliant with this policy may be blocked or restricted. A particular website that is deemed acceptable for use may still be judged a risk to the District (*e.g.*, it could be hosting malware, etc.), in which case it may also be subject to blocking or restriction. Any attempt to circumvent or disable Internet blocking will result in immediate termination of network privileges.

The District also retains sole discretion to use hardware or software that screens e-mails for harmful or potentially dangerous content. E-mail messages that contain harmful or potentially dangerous content will not be delivered to or from District Users.

No Expectation of Privacy: Users have no expectation of privacy in their use of District Technology. Log files, audit trails and other data about User activities with District Technology may be used for forensic training or research purposes, or as evidence in a legal or disciplinary matter. Users are on notice that District Technology is subject to search and seizure in order to facilitate maintenance, inspections, updates, upgrades, and audits, all of which necessarily occur frequently and without notice so that the District can maintain the integrity of District Technology. All data viewed, created, saved, accessed, or stored on District Technology is subject to monitoring, inspection, review, copying,

modification, deletion, audit, disclosure and discovery. Such data may be subject to disclosure pursuant to the Public Records Act (California Government Code section 6250, *et seq*.). Pursuant to the Electronic Communications Privacy Act of 1986 (18 USC 2510, *et seq*.), notice is hereby given that there are no facilities provided by District Technology for sending or receiving private, except as permitted under "Personal Use" (above), or confidential electronic communications. System Administrators have access to all e-mail and will monitor messages. Messages relating to or in support of illegal or inappropriate activities will be reported to the appropriate authorities and/or District personnel.

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. Users should be aware that, in most instances, their use of District Technology (such as web searches or e-mails) cannot be erased or deleted. Accordingly, any such information may be accessed by the District and may potentially be subject to subpoena, discovery in litigation, or responsive to a Public Records Act request. The District reserves the right to review any usage and make a case-by-case determination whether the User's duties require access to and/or use of District Technology which may not conform to the terms of this policy.

Specific Consent to Search and Seizure of District Technology: The undersigned consents to the search and seizure of any District Technology in the undersigned's possession by the District, the District's authorized representative, a System Administrator, or any Peace Officer. This consent is unlimited and shall apply to any District Technology that is in the possession of the undersigned, whenever the possession occurs, and regardless of whether the possession is authorized.

Disclaimer Notice in District E-mail

The following disclaimer shall be added by the District to each outgoing e-mail:

> This e-mail and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this e-mail in error please notify the system administrator. Please note that any views or opinions presented in this e-mail are solely those of the author and do not necessarily represent those of the District. Finally, the recipient should check this e-mail and any attachments for the presence of viruses. The District accepts no liability for any damage caused by any virus transmitted by this e-mail.

Attorney-Client Privileged Communications

Some of the messages sent, received or stored on the District electronic message system will constitute confidential, privileged communications between the District and its attorneys. Upon receipt of a message either from or to counsel, Users should not forward it or its contents to others inside the District or any other person outside the District without counsel's express authorization. Upon learning that a privileged and/or confidential communication has been received by or sent to any individual not

intended to receive such a communication, Users must immediately notify the Superintendent so that he/she may take appropriate steps to preserve the privilege.

California Public Records Act Request ("CPRA")/Litigation

The CPRA (Government Code section 6251, *et seq*.) is a law that requires inspection and/or disclosure of governmental records to the public upon request. E-mails sent by Users, unless otherwise exempt by law, are subject to inspection and disclosure under the CPRA by any person making such a request.

Furthermore, e-mails may also be subject to discovery and disclosure as a result of pending litigation involving the District, the District's Employees and elected or appointed officers or officials.

Searching Personal Devices and Accounts for Disclosable Records: Employees using personal electronic devices or accounts to send or receive communications constituting District-related business may be required to search their personal electronic devices and accounts for potentially disclosable records pursuant to a request made under the CPRA. Communications constituting District-related business are those communications that relate in a substantive way to the conduct of the District's business. Communications that are primarily personal in nature or that contain no more than incidental mentions of the District's business may not constitute District-related business communications.

Searches of personal electronic devices and accounts by an employee shall be conducted during the employee's regular work hours.

The Superintendent or designee shall promptly notify an employee of the District's receipt of a CPRA request that may implicate District records located on the employee's personal devices or accounts and shall provide the employee with instructions for conducting such searches that identify the specific type and nature of records for which the employee is required to search and collect, as well as the specific type and nature of records that may be withheld because they are not District-related business.

Following an employee's search of their personal electronic devices or accounts, the employee shall be required to sign an affidavit reporting the results of the search and the factual basis for withholding any otherwise disclosable records, and attesting, under penalty of perjury, that the employee has searched for and collected all potentially disclosable records pursuant to the relevant PRA request, and that all other information set forth in the affidavit is true and correct.

Alternatively, an employee may choose to have the District perform the search of the employee's personal electronic devices and accounts.

Security

All data must be kept confidential and secure by the Employee. The fact that the data may be stored electronically does not change the requirement to keep the information confidential and secure. Rather, the type of information or the information itself is the basis for determining whether the data must be kept confidential and secure. If this data is stored in a paper or electronic format, or if the data is copied, printed, or electronically transmitted, the data must still be protected as confidential and secured. Users

are responsible for keeping their District Technology secure from access by any unauthorized Users. Computers should not be left unlocked and logged into by staff in the vicinity of students or the public. All Users are expected to take reasonable precautions as prescribed by District IT staff to prevent the spread of computer viruses, malware, etc.

Definitions

Blogging
An online journal that is frequently updated and intended for general public consumption.

E-mail
The electronic transmission of information through a mail protocol, such as SMTP or IMAP. Typical e-mail programs include Microsoft Outlook.

Chain E-mail
E-mail sent to successive people. Typically, the body of the note has directions to the reader to send out multiple copies of the note so that good luck or money will follow.

District Technology
All technology owned or provided by the District to authorized Users, including Internet/Intranet/Extranet-related systems, computer hardware, software, Wi-Fi, electronic devices such as tablet computers, USB drives, cameras, smart phones and cell phones, telephone and data networks (including intranet and Internet access), operating systems, storage media, wireless access points (routers), wearable technology, PDA's, network accounts, web browsing, Blogging, social networking, and file transfer protocols, e-mail systems, electronically stored data, websites, web applications or mobile applications, 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
Any individual employed by the District or its affiliated agencies or departments in any capacity, whether full or part-time, active or inactive, including interns, contractors, consultants and vendors.

Flaming
The use of abusive, threatening, intimidating, or overly aggressive language in an Internet communication.

Hacking
Gaining or attempting to gain unauthorized access to any computer systems, or gaining or attempting to gain unauthorized access to District Technology.

Harassment
The persistent annoyance of another User, or interference with another User's work, including, but not limited to, the sending of unwanted e-mail.

Instant Messaging

A type of communications service that enables the creation of a kind of private chat room with another individual in order to communicate in real time over the Internet.

Internet Resources
Websites, Instant Messaging applications, file transfer, file sharing, and any and all other Internet applications and activities using either standard or proprietary network protocols. Examples of websites that pose a risk to the District, or are counter to its mission, are malware repositories, sites advocating violence against civil society or against persons based on race, religion, ethnicity, sex, sexual orientation, color, creed or any other protected categories, sites offering gambling activities or that are pornographic in nature.

IP Address
Unique network address assigned to each computing device connected to a network to allow it to communicate with other devices on the network or Internet.

Malware
Any software, application, program, e-mail or other data or executable code which is designed to cause harm to a network or computer or violate any law, statute, policy or regulation in any way. Examples of harmful activity or intent are theft of personal information or intellectual property by Phishing or other means, hacking, violation of copyright law (distributing or copying written material without proper authorization), propagation of Spam e-mails, harassment, extortion, denial of service and facilitating access to illegal content (pornography, gambling, etc.). Accessing or storing malware is expressly prohibited unless authorized for research or forensic purposes by appropriately authorized and designated Employees.

Network
Any and all network and telecommunications equipment, whether wired or wireless, controlled or owned by the District which facilitate connecting to the Internet.

Phishing
Attempting to fraudulently acquire Sensitive Information by masquerading as a trusted entity in an electronic communication.

Sensitive Information
Classified as Protected Health Information (PHI), Confidential Information or Internal Information.

Spam
Unsolicited nuisance Internet E-mail which sometimes contains malicious attachments or links to websites with harmful or objectionable content.

Spoofing
The act of replacing IP address information in an IP packet with falsified network address information. Each IP packet contains the originating and destination IP addresses. By replacing the true originating IP address with a falsified address a hacker can obscure their network address and hence, the source of a network attack, making traceability of illegal or illegitimate Internet activity extremely difficult.

System Administrator
District Employees whose responsibilities include District Technology, site, or network administration. System Administrators perform functions including, but not limited to, installing hardware and software, managing a computer or network, auditing District Technology, and keeping District Technology operational.

Unauthorized Disclosure
The intentional or unintentional act of revealing restricted information to people, both inside and/or outside the District, who do not have a need to know that information.

User or Users
Individual(s) whether students or Employees, full or part-time, active or inactive, including interns, contractors, consultants, vendors, etc. who have used District Technology, with or without the District's permission.

User ID
Uniquely assigned Username or other identifier used by an Employee to access the District network and systems.

Vandalism
Any malicious attempt to harm, modify, or destroy data of another User on the District network, or other networks that are connected to the Internet, or tampering with any part of the network which a User has not been granted permission to access. This includes, but is not limited to, the uploading or creating of computer viruses, deleting or modifying files, or changing system settings.

Merced City School District

Employee Technology Acceptable Use Agreement

Acknowledgment of Receipt & Agreement

I have received, read and understand, this Employee Technology Acceptable Use Agreement, dated 05/14/2024, revised 06/05/2024 and agreed upon by MCTA and CSEA. I agree to abide by the Agreement, Board Policy and Administrative Regulation 4040 - Employee Use of Technology, and other applicable laws and District policies and regulations governing the use of District Technology. I understand that any violation of those legal sources may result in revocation of my User privileges, disciplinary action, and/or appropriate legal action. I further understand that there is no expectation of privacy when using District Technology or when using my personal electronic device with District Technology.

I hereby release the District, its Board, agents and personnel from any and all claims and damages arising from my use of District Technology or from the failure of any service or technology protection measures employed by the District or by MCOE.

Name: (Please print) _____ Position:_____

School/Work Site:_____

Signature: _____ Date:_____

Board Approved: 05/14/2024
Revised: 06/05/2024