

EMPLOYEE USE OF TECHNOLOGY**NORTH MONTEREY COUNTY UNIFIED SCHOOL DISTRICT
ACCEPTABLE USE AGREEMENT
AND RELEASE OF DISTRICT FROM LIABILITY (EMPLOYEES)**

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 North Monterey County Unified School District (“District”) recognizes and supports advances in technology and provides an array of technology resources for employees to use to enhance 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.

Pursuant to District Policy, 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.

Terms of Use

Acceptable Use: North Monterey County Unified School 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 Agreement or other North Monterey County Unified School District policies. The District reserves the right to restrict online destinations through software or other means.

Additionally, the North Monterey County Unified School District expressly prohibits:

1. Using District Technology for commercial gain;
2. Accessing District Technology for the purpose of gaming or engaging in any illegal activity;
3. Transmission of confidential information to unauthorized recipients;
4. Inappropriate and unprofessional behavior online such as use of threats, intimidation, bullying or “flaming”;
5. Viewing, downloading, or transmission of pornographic material;
6. Using District Technology for the creation or distribution of chain emails, any disruptive 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;
7. Significant consumption of District Technology for non-business related activities (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);

8. 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;
9. Using copyrighted information that violates that copyright; or
10. 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 in with their uniquely assigned North Monterey County Unified School 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.

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 email) 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.

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 makes no warranties (expressed or implied) with respect to: (a) the content of any advice or information received by an employee, or any costs or charges incurred as a result of seeing or accepting any information; or (b) any costs, liability, or damages caused by the way the employee chooses to use his or her access to the network.

Password Policy: Passwords must not be shared with anyone and must be treated as confidential information. Passwords must be changed at least every 180 days. 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.

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

Revocation of Authorized Possession: 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.

Third-Party Technology: Connecting unauthorized equipment to the District Technology, including the unauthorized installation of any software (including shareware and freeware), is prohibited.

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: 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 web site that is deemed “Acceptable” for use may still be judged a risk to the District (e.g. it could be hosting malware), in which case it may also be subject to blocking or restriction.

No Expectation of Privacy: Users have no expectation of privacy regarding 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. 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 or confidential electronic communications. System Administrators have access to all email 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.

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 at any time of the day or night and by any means. 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. The undersigned waives any rights that may apply to searches of District Technology under SB 178.

Consequence of Policy Violation: Users found to be in violation of this policy may be subject to discipline up to and including termination.

Justifiable, Work-Related Usage

The North Monterey County Unified School 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.

Disclaimer Notice in District Email

The following disclaimer will be added to each outgoing email:

“This email 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 email in error please notify the system administrator. Unless you are the addressee (or authorized to receive messages for the addressee), you may not use, copy, disclose, or distribute this message (or any information contained in or attached to it) to anyone. You may be subject to civil action and/or criminal penalties for violation of this restriction. Please note that any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the District. Finally, the recipient should check this email and any attachments for the presence of viruses. The North Monterey County Unified School District accepts no liability for any damage caused by any virus transmitted by this email.”

California Public Records Act Request (“CPRA”)/Litigation

CPRA outlined in Government Code section 6251 et seq. is a law that requires inspection and/or disclosure of governmental records to the public upon request. Emails sent by employees, unless otherwise exempt by law, are subject to inspection under the CPRA by any person making such a request.

Furthermore, emails may also be subject to disclosure as a result of pending litigation involving the District, the District’s employees and elected or appointed officers or officials.

It is the District’s policy that District email and email systems are intended to be a medium of communication. District email systems are not intended to be, and may not be used for, the electronic storage or maintenance of District records. The email system, to function as intended, anticipates or requires that employees regularly delete communications from the system.

Email messages and attachments comparable to hard copy documents that would be retained under this policy should be retained as follows: The document must be categorized in the appropriate record series and converted to the appropriate electronic format or printed in hard copy and retained for the required time period as outlined in the District’s Records Retention/Disposition Schedule. No matter what form in which the record is retained, proper procedures as outlined in the District’s Records Retention Policy must be followed prior to the destruction of any record.

Routine email messages comparable to telephonic communications are non-records. They are not intended to be retained in the ordinary course of District business, and the informational content of such communications is neither necessary nor intended to be preserved for future District use or reference. Each employee will have the responsibility to remove such non-records from folders within the District’s electronic mail system on a rolling ninety (90) day schedule. This includes items in “received” and “sent” folders as well as any folders set up by individual users. Upon removal from the District’s email system the non-records will be disposed of in the District’s ordinary course of business. An email is considered destroyed as soon as it has been deleted from a user’s mailbox, even though it is temporarily stored in the trash folder before being purged from the email system. This action is analogous to throwing a

paper document into an office trash can. Digital email backup servers and or tapes are re-written over as space is need in order for the system to function properly and efficiently.

Each email user will be trained in the application and implementation of this policy.

This policy does not prohibit employees from maintaining temporary working files or folders to allow for quick reference to recent emails.

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.

All software programs, applications, source code, object code, documentation and data shall be guarded and protected.

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 clients 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.

Employee

Any individual employed by the North Monterey County Unified School 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.

District Technology

Internet/Intranet/Extranet-related systems, including but not limited to, computer hardware, software, Wi-Fi, electronic devices such as tablet computers, cameras, smart phones and cell phones, telephone and data networks (including intranet and Internet access), operating systems, storage media, PDA's, network accounts, web browsing, blogging, social networking, and file transfer protocols, email systems, and electronically stored data, websites, web applications or mobile applications, provided by the District to authorized users to facilitate the completion of their jobs.

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

Web sites, 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 web sites 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

Malware is any software, application, program, email 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 North Monterey County Unified School 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

Spam is unsolicited nuisance Internet E-mail which sometimes contains malicious attachments or links to web sites with harmful or objectionable content.

Spoofing

IP Address spoofing is 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, 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 been given access to and granted permission(s) to use District Technology.

User ID

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

Acknowledgement of Receipt & Agreement

I acknowledge that I have received, read and understood the North Monterey County Unified School District Acceptable Use Agreement and Release of District from Liability (Employees), as revised October 6, 2016. I understand that any violations of the Agreement may be grounds for disciplinary action, up to and including termination. I understand that a copy of the signed Acceptable Use Agreement will be placed in my personnel file.

Signature

Date

Print Name