COAST UNIFIED SCHOOL DISTRICT

ACCEPTABLE USE
OF TECHNOLOGY AGREEMENT

The purpose of this Employee Acceptable Use of Technology Agreement ("Agreement") is to ensure a safe and appropriate environment for all employees and students. Pursuant to Board Policy ("BP") 4040, this Agreement notifies staff about the acceptable ways in which District Technology may be used at Coast Unified School District ("District") and how all technology may be used without violating student privacy laws. The District recognizes and supports advances in technology and provides an array of technology resources for employees to use to enhance the learning environment, 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 Board Policy, only employees who submit a signature acknowledging receipt and agreement to the terms of use outlined in this Agreement are authorized to use District's Technology. (See e.g., BP 4119.21, 4219.21, 4319.21—Professional Standards; AR 4218—Dismissal/Suspension/ Disciplinary Action; BP/AR 4118—Suspension/ Disciplinary Action; BP 4040—Employee Use of Technology; BP/AR 6163.4—Student Use of Technology.)

I. Definitions

A. "District Technology" is defined as all District owned and maintained, created or authorized electronic technology including, but not limited to, computer hardware and software, electronic devices such as tablet computers, smart phones and cell phones, telephone and data networks (including intranet and Internet access), 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. The definition of District Technology expressly includes access to District data networks from devices owned by a User or the District, whether on or off District property.

B. "Employee" for the purposes of this acceptable use agreement, means any individual employed by theDistrict or its affiliated agencies or departments in any capacity, whether full or part-time, active or inactive, includinginterns, contractors, consultants, vendors or Board Members.

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

D. "System Administrator" means the Superintendent or designee and staff employed by the District and persons employed by District departments 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.

E. "User" or "Users" means someone who uses District Technology, but does not have System Administrator responsibilities.

F. "User Account" means the combination of a User number, User name, and/or User ID and a password that allows an individual User access to District Technology.

II. District Rights and Responsibilities

It is the policy of the District to maintain an environment that promotes ethical and responsible conduct in all online network activities by employees. Employees shall not have an expectation of privacy when using District Technology, or personal technology, to access the District's network. It shall be a violation of this policy for any employee to engage in any activity that does not conform to the established purpose, and general rules and policies of the network. The District retains the following rights and recognizes the following obligations:

1. To monitor employee use of District Technology to ensure public resources are appropriately used and to ensure that the District's policies and regulations regarding harassment and nondiscrimination, as well as other applicable policies and regulations, are being followed. The District can and does monitor District Technology access and activity, including but not limited to, websites visited, content viewed, information posted, applications run, content created and stored, and email sent and received. This monitoring includes User access to private online accounts through the District Technology. The District reserves the right to access, and view, any material accessed or stored on District Technology or any material used in conjunction with District Technology, even if that material is stored on a device that is not owned by the District. Electronically generated content produced by District employees may also be subject to the California Public Records Act, and may be subject to public disclosure.

2. To log network use and to monitor and maintain fileserver space utilization by Users. The District does not assume responsibility or liability for files deleted due to violation of fileserver space allotments. Should a User's files be deleted by a System Administrator, the District shall not be liable for the deletion. Users are encouraged to back up important documents via an external drive or device.

3. To remove a User account on the network.

4. To provide guidelines and make reasonable efforts to train employees in acceptable use and policies governing online communications.

5. 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 District Technology,

including but not limited to District email, and will monitor messages sent through District Technology. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.

6. To provide internal and external controls as appropriate and feasible. Such controls shall include the right to determine who will have access to District Technology and, specifically, to exclude those who do not abide by the District's terms of use or other policies governing the use of school facilities, equipment, and materials. The District reserves the right to restrict online destinations, accessed through District Technology, through software or other means.

7. User files and information on District Technology may be subject to search or seizure by law enforcement agencies for investigations if such files contain information which may be used as evidence in a court of law.

8. 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. Upon the loss of authorized use of District Technology, Users must immediately surrender, to the District, any and all District Technology and User Account information. The loss of authorization to use District Technology expressly, and immediately, rescinds the User's status as an "authorized possessor" as defined in Penal Code section 1546.

III. Employee Responsibilities and Terms of Use

Retention of Records

Users shall, as a condition of using District Technology, read and adhere to the requirements of all Board Policies and Administrative Regulations concerning the handling of student records, District information and the use of District Technology, including but not limited to the following:

1. Access to District Records (see BP 1340; and AR 1340.)
2. Retention of Electronic Records (see BP 3580; and AR 3580 – District Records.)
3. Public Records and Retention of Electronic Records (see BP 4040 – Employee Use of Technology.)
4. Board Member Electronic Communications (see BP 9012.)

Pursuant to these polices, and regulations, Users are directed to manage their email accounts in accordance to District policy, and regularly transfer District information to the appropriate location, and purge non-District related information from their email accounts. Additionally, employees who use their personal devices, or accounts, to conduct District business, may be required to search their personal devices, or accounts, in accordance with state law in order to provide the District with its records, or information. Employees who are directed to search their personal devices, or accounts, must do so only in the manner described by District policy, or as directed by the Superintendent, or designee. Please refer to these District policies and regulations for specific guidelines.

Attorney-Client Privileged Communications

Some of the messages sent, received or stored on District Technology will constitute confidential, privileged communications between the District and its attorneys. Upon receipt of a message either from or to counsel, employees should not forward it or its contents to others inside the District or any other person outside the District without counsel's express authorization.

Activities deemed to be appropriate uses of District Technology include the following:

A. Instructional Use:

1. Use in classroom instruction.
2. Development of instructional materials.
3. Research connected to academic, and instructional concerns and interests.
4. Communication with colleagues, students, and professional organizations and institutions if such communications are related to the business of the District.

B. Administrative Use:

1. District administrative and business communications and transactions.
2. Communication with colleagues, students and professional organizations and institutions if such communications are related to the business of the District.
3. Research tied to District concerns and interests.

C. Incidental Personal Use: The District's Technology, including Internet access, are to be used primarily for educational purposes and District business. Staff may use the District's Internet access subject to the following limitations:

1. Incidental personal use is limited to off-duty time except in cases of emergency.
2. Incidental use of District Technology by employees does not extend to family members or other acquaintances who are not employed by the District.
3. Incidental use must not result in direct costs, or liability, to the District.
4. Incidental use must not interfere with the normal performance of an employee's work duties or student learning.
5. Incidental use must not violate this Agreement.

Inappropriate use of District Technology includes, but is not limited to, the following:

A. Any use of the District's Technological resources for illegal and/or unauthorized purpose is prohibited.

B. Using District Technology to access or view pornography.

C. Disclosing any student's personally identifiable information. Federal and California law prohibit the District's employees from disclosing a student's personally identifiable information using any means including, but not limited to, District Technology, personal technology or by requiring students to use technology in connection with a classroom assignment or extracurricular activity without prior, written parental consent. (20 U.S.C. § 1232g; Ed. Code, § 49076, subd. (a).)

Examples of technology that may disclose a student's personally identifiable information include, but are not limited to, cell phone text messaging, email, iPhone's iMessage, Facebook, Facebook Messenger, Twitter, Instagram, Pinterest, YouTube, LinkedIn, Flickr, Tumblr, Vine, Podcasts, Google Plus +, Google Chat, Skype, online chat rooms, Snapchat, WhatsApp, Weebly, Wix and Prezi, or similar electronic application or social media platforms.

District employees are prohibited from entering into an agreement with any third-party provider of technology that grants the third-party provider access to a student's personally identifiable information without the prior, written permission of the Superintendent or designee.

"Personally identifiable information" includes, but is not limited to, the following:

a. Student's name.
b. Student's photograph.
c. A video featuring a student.
d. Name of the student's parent or other family members.
e. The address of the student or student's family.
f. A personal identifier such as the student's social security number, student number, or biometric record.
g. Indirect identifiers such as the student's date of birth, place of birth, and mother's maiden name.
h. Other information that alone or in combination, is linked or linkable to a specific student which would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances to identify the student with reasonable certainty.

District employees are prohibited from releasing personally identifiable information regarding a student even when the employee reasonably believes that the person requesting information knows the identity of the student he or she is requesting information about. (Ed. Code, § 49061; 34 C.F.R. § 99.3.)

D. Posting or identifying students via social media without written permission by the District and the student's parent/guardian.

E. Using District Technology to gain or attempt to gain unauthorized access to any computer technology, or gaining or attempting to gain unauthorized access to District Technology is prohibited.

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

G. Unauthorized attempts to circumvent data protection schemes or uncover security loopholes within or outside of District Technology are prohibited. This includes creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secure data.

H. 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.

I. Knowingly or carelessly accessing, transmitting, downloading, tampering, vandalizing, running or installing on any District Technology, or giving to another User, a program or file intended to damage or to place excessive load on a computer technology or network, files or data is prohibited. This includes, but is not limited to, programs known as computer viruses, Trojan Horses, worms, or any type of pyramid schemes. Deliberate attempts to degrade or disrupt technology performance of the network or any other computer technology or network on the Internet by spreading computer viruses is considered criminal activity under state and federal law.

J. Violating terms of applicable software licensing agreements or copyright laws on District Technology is prohibited. Downloading, copying, otherwise duplicating, and/or distributing copyrighted materials without the specific written permission of the copyright owner is prohibited, except that duplication and/or distribution of materials for educational purposes is permitted when such duplication and/or distribution would fall within the Fair Use Doctrine of the United States Copyright Law. Employees should seek written permission from the Superintendent or designee prior to duplicating and/or distributing copyrighted materials.

K. Using District Technology for commercial activity or for-profit purposes, such as creating products or services for sale, or advertising/promoting non-district sites, commercial efforts and/or events, soliciting votes, or political lobbying is prohibited.

L. Inappropriate mass mailing via District Technology is prohibited. This includes multiple mailings to newsgroups, mailing lists, or individuals, (e.g. “spamming,” “flooding,” or “bombing”). This also includes initiating or propagating electronic chain emails via District Technology.

M. Forging the identity of other Users' names, emails, files, data or machine in an electronic communication via District Technology in any way, including, but not limited to, disguising one's identity, impersonating other Users, or sending anonymous email is prohibited. Real names must be used; impersonation and pseudonyms are not allowed.

N. Knowingly or recklessly posting, transmitting or reproducing materials that are false, slanderous or defamatory about a person or organization, or that otherwise violates existing laws or regulations by using District Technology is prohibited.

O. Attempting to monitor or tamper with another User's electronic communications, or reading, copying, changing, or deleting another User's files or software via District Technology, without the explicit agreement of the owner, is prohibited.

P. Pirating of computer software via District Technology is prohibited.

Q. Selling, purchasing or encouraging the use of drugs, alcohol or tobacco or other illegal items or substances is prohibited.

R. Intentionally accessing, creating, storing, posting, submitting, displaying, transmitting, using or downloading material, images or language that may be deemed hate mail, profane, lewd, vulgar, rude, inflammatory, disrespectful, abusive, impolite, threatening, harassing, discriminatory, racist, offensive, indecent, obscene, or intimidating is prohibited.

S. Malicious use of District Technology to develop programs that harass others or infiltrate a computer or computing technology and/or damage software components of a computer or computing technology, and/or "hacking" internal or external to the District, or attempting to access information protected by privacy laws, is prohibited.

T. Use of District Technology for non-academic related bandwidth intensive activities, such as network gaming, is prohibited.

U. District Technology such as, but not limited to, hardware and/or software shall not be destroyed, modified, or abused in any way.

V. District Technology may not be used for downloading entertainment software (or other files not related to the mission and objectives of the District) for transfer to a User's home computer, personal computer, or other device.

W. Establishing a network of Internet connections to live communications, including voice and/or video (relay chat), unless specifically authorized by a System Administrator, is prohibited.

X. Using District Technology to engage in personal attacks, including prejudicial or discriminatory attacks such as "cyberbullying" is prohibited.

Y. Using District Technology to violate any criminal laws, federal, state or municipal laws or ordinances, as well as board policy is prohibited.

Z. Any use of District Technology to send or receive a message that is inconsistent with the school's code of conduct is prohibited.

AA. Creation of websites, blogs or other Internet forums that purport to be or hold themselves out to be District-sponsored without prior written permission from the Superintendent or designee. In deciding whether to grant such approval, the Superintendent or designee may ask for the purpose of the particular use of technology, the proposed content, the person designated to maintain the site, any links which may be contained on the site, and privacy settings.

IV. Disclaimer

The District cannot be held accountable for the information that is retrieved via the network or District Technology. 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 Technology, System Administrator or your own errors or omissions. Use of any information obtained via District Technology 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 a User, 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 User chooses to use his or her access to the District Technology.

V. Email

Email, which is subset of District Technology, is an important communication tool utilized by employees. However, misuse of email can pose many legal, privacy and security risks. Thus, it is important for employees to understand the appropriate use of electronic communications using the District's email. All employees must adhere to the District's rules and regulations, as outlined in this policy, regarding email.

A. <u>No Expectation of Privacy</u>

The District owns any communication sent via email or that is stored on District Technology. Specifically, employees should have no expectation of privacy when using the District's email system. The District will monitor all email use to ensure compliance with this policy. Therefore, the use of the District's email system constitutes express consent for the District to monitor and/or inspect any data that employees create or receive, or any messages sent or received. Employees should not consider any incoming or outgoing email communications to be private.

B. Inappropriate Use

Generally, an employee's use of email must adhere to professional standards guidelines. Employees are prohibited from sending jokes, pictures, or forms via email that violate the District's discrimination or harassment policies. Specifically, employees must not recklessly post, transmit or reproduce materials that are false, slanderous or defamatory about a person or organization, or that otherwise violate existing laws or regulations by using District Systems.

VI. Security

All data must be kept confidential and secure by the User. 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.

VII. Password Policy

User Accounts such as, but not limited to, 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.

VIII. 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 pursuant to the Electronic Communications Privacy Act (Pen. Code, § 1546 et seq.).

IX. Consequence of Policy Violation

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

X. Acknowledgement of Receipt & Agreement

By signing the Annual Employee Information Packets Employee Acknowledgement I acknowledge that I have read and understand this Acceptable Use of Technology Agreement. I understand that any violations of the Agreement may be grounds for disciplinary action, up to and including termination.