

Technology Acceptable Use and Security Policy

The Technology Acceptable Use and Security Policy (“policy”) applies to all CUSD employees and any other person or entity granted access to or use of the District’s computer network and facilities, whether or not employed by the District (“Users”).

To gain access to District computers, facilities, network, software applications, and the Internet, Users must review and agree to abide by the terms of this CUSD Technology Acceptable Use and Security Policy.

1. Educational and Business Objectives. District computers, networks, software applications, electronic mail, voice mail and other computer, electronic and telecommunication technologies and facilities are to be used solely for CUSD business and educational purposes.

Coast Unified School District is committed to making advanced technology and increased access to learning opportunities available to students, faculty, and other district employees. The district’s goal in providing this access is to promote educational excellence in schools by facilitating resource sharing, innovations, and communications. To be in compliance with the Children’s Online Privacy Protection Act (COPPA) and the Children’s Internet Protection Act (CIPA) as mandated by Congress, Coast Unified School District has implemented the following guidelines and procedures for using the Internet. This Acceptable Use Policy and Media Consent form is a legally binding document.

CIPA mandates school districts to certify that they have in place an Internet Safety Policy. These mandates and assurances must be in place in order to receive E-rate funds or funds under Title III of Elementary and Secondary Education Act of 1965. Coast Unified School District incorporates Internet filtering technology, remote monitoring technology, network transaction auditing and staff supervision to prohibit obscenity, child pornography and material harmful to minors in compliance with CIPA.

COPPA applies to the online collection of personal information from children under 13. School districts must be COPPA compliant order to receive E-rate funds. Coast Unified School District does not disclose personal information about students on district websites or through any unsecured Internet communication and staff members are instructed not to allow students to enter personal information on any external website or through any other Internet communication in compliance with COPPA. A consent form must be signed prior to any personal student information or work being placed on any district provided website.

2. CUSD Property. All technology devices, software, and equipment configurations are owned by the Coast Unified School District. All files stored on CUSD equipment and back-up devices are considered to be property of the CUSD, and materials developed by staff in the course of carrying out their professional responsibilities on District time shall be the property of CUSD. All equipment, software and business files must be returned immediately upon termination of employment.

Neither the hardware nor software configuration can be changed without specific permission from the Technology Department. Examples of changes requiring authorization include: installing new software or hardware, formatting a hard drive, adding new drivers. To request a change, submit a Service Request to the Technology department. Any intentional damage to the configuration of equipment may result in appropriate disciplinary actions.

If the technology issued to a User is stolen, whether on CUSD property, or in the User’s personal possession, the User is responsible to immediately notify the police and a copy of the report must be submitted to the proper CUSD personnel. All required equipment and software repairs should be reported to the Help Desk through the Service Request System and repaired only by authorized CUSD personnel.

3. Use Is A Privilege

Use of the District's computing and networking resources is a privilege. The CUSD and the individual schools reserve the right to restrict or terminate network and Internet access at any time. *Any student, district employee, staff member or user identified as a security risk may be denied access.*

4. No Expectation of Privacy. USERS OF THE CUSD COMPUTER NETWORK SYSTEM (INCLUDING BUT NOT LIMITED TO EMAIL AND THE INTERNET) HAVE NO EXPLICIT OR IMPLICIT EXPECTATION OF PRIVACY. Any or all uses of the system and all files on the system may be intercepted, recorded, monitored, copied, deleted, audited, inspected and disclosed to authorized personnel as well as any other person or entity permitted access under the law. CUSD shall cooperate with law enforcement agencies investigating illegal activity on the CUSD network.

Unless otherwise stated, submission of a HelpDesk call or Service Request will authorize technicians to access individual's e-mail or files as it may be necessary for technical support personnel to review the information during the course of problem resolution.

5. User Back-up. It is the user's responsibility to back up critical business data and files.

6. Internet Service Providers. While on an CUSD site, staff must access the Internet only through the CUSD's network. All Internet traffic must pass through the CUSD network where access controls and related security mechanisms will be applied. Staff may not use any service to bypass the CUSD network, security mechanism, or content filtering policies.

7. Safety. Sharing of personal information via the Internet such as name, address, and phone number, can compromise personal safety. Privacy cannot be guaranteed in a network environment. *Student/teacher relationships on Facebook and other social networking sites are strongly discouraged.*

8. Confidentiality of Information. CUSD staff may have access to information which is confidential. CUSD requires that staff maintain absolute confidentiality in all electronic student, employee, and application matters. Access to confidential information REGARDING DISTRICT STAFF OR STUDENTS is authorized ONLY when staff have a legitimate business need to access the information to fulfill his or her professional responsibility, and for which they have been explicitly authorized to access. UNAUTHORIZED ACCESS TO OR DISSEMINATION OF CONFIDENTIAL INFORMATION SHALL BE GROUNDS FOR DISCIPLINE UP TO AND INCLUDING TERMINATION.

9. Liability. The CUSD makes no assurances of any kind, expressed or implied, regarding any computer or Internet services provided.

10. Appropriateness of Materials. Access to the Internet provides opportunities for staff and students to explore resources outside of the walls of their schools or offices. The CUSD acknowledges the fact that inappropriate materials exist and will make what it judges to be reasonable and appropriate efforts to avoid such materials, including the use of filtering software. However, no software or appliance can filter out all materials that are inappropriate or unacceptable for academic purposes and it should be clearly understood by all staff, students, and students' parents/guardians that intentional access to such material, in any form, is strictly forbidden. The network is designed to achieve and support the CUSD's business and instructional goals and any information that does not support the goals is to be avoided. *Users will immediately report to a supervisor an obscene, pornographic, or offensive material found.* If a staff or student unintentionally accesses such information while doing legitimate research, he/she should contact the person responsible for technology at his/her site for appropriate action. It is the responsibility of all users, staff and students, to ensure that CUSD computers, the network, and the Internet are being used for educational or CUSD business purposes.

Due to bandwidth restrictions, students are prohibited from downloading and/or listening to radio streaming, video streaming, using any online telephone resource, or sharing music and/or video.

Users shall not download or install from other sources any non-curriculum software unless approved by a principal or network administrator. This includes, but not limited to, non-educational games, peer-to-peer file-sharing software, remote control software, optimizing utilities, networking utilities, shareware software, freeware software, and Internet messengers. All software installed on district computers must be licensed and approved. Pirated software will not be tolerated.

11. Copyright. Unless it is otherwise stated, Users should assume that all materials on the Internet, including web sites and graphics, are copyrighted. Existing copyright guidelines, such as those involving photocopying, multimedia, and fair use, apply. Copyrighted material shall be posted online only in accordance with applicable copyright laws. Staff and students may not copy software on any CUSD computer and may not bring software from outside sources for use on CUSD equipment without the prior approval of the Technology Department or its designee. The District shall not be responsible or liable for unauthorized use or distribution of copyrighted materials and reserves the right to seek indemnification from the user for the inappropriate use, distribution or possession of copyrighted material on the District computers or network facilities.

12. Security and Passwords:

- A User in whose name a network account is issued is responsible at all times for its proper use, and such User shall access the system only under the account number that has been assigned to him/her.
- Passwords must never be shared. To share a User ID or password exposes the authorized User to responsibility for actions the other party takes with the password and ID.
- Users must take reasonable steps to ensure the security/privacy of their passwords, including changing the password periodically, selecting a password that is complex and known only to the User, and never displaying the password in a public place.

13. Security and Connectivity

- *Any use of personal laptops by faculty, staff or students that is to be used with Coast Unified School District must be checked by the Technology Department in order to be on school premises.*
- Users may not make arrangements for, or complete the installation of, any physical or logical connection, nor make alterations to the existing CUSD network unless approved by the Technology department. This includes connecting computers, servers, network electronics or other network enabled devices to the CUSD's network.
- Users may not establish any physical or logical network connection that could allow users to gain unauthorized access to the CUSD's systems and information. This includes the establishment of multi-computer file systems, web services, Internet, and FTP servers.
- Users may not establish any unauthorized server or file sharing mechanism, including, but not limited to, intranet servers, electronic bulletin boards, instant messaging, local area networks, modem connections to existing networks, or multi-user systems for communicating information.
- No proxies or personal firewalls are allowed.

14. Use of Wireless Devices. PDAs, Pocket PCs, cellular phones, and other wireless devices that can contain sensitive information must be secured in the same manner as desktop and laptop computers. These devices will be issued and returned according to CUSD equipment procedures. If equipment issued to a user is lost or stolen, it is the User's responsibility to report the loss immediately. Failure to take reasonable and appropriate steps to secure sensitive information shall be grounds for discipline, including possible termination.

15. Appropriate Behavior. Staff members are responsible for appropriate behavior on the CUSD's computers, business systems, network, and the Internet, and must adhere to all relevant federal, state, and local laws, as well as CUSD policies and procedures. Users who disregard these requirements and guidelines may have their privileges suspended or revoked, and disciplinary action taken against them, including termination.

Users granted access to the network through the CUSD's computers assume personal responsibility and liability, both civil and criminal, for uses of the network not authorized by this policy and the CUSD's guidelines. The district does not sanction any use of its computer systems or the Internet that is not authorized by or

conducted strictly in compliance with this policy. The CUSD retains the right to remove from its information systems any material it views as offensive or potentially illegal.

The CUSD declares unethical and unacceptable behavior as just cause for disciplinary action up to and including termination of employment, the revocation of network access privileges, and/or the initiation of legal action for any activity through which an individual:

1. Uses the CUSD's computers and/or network for illegal, inappropriate, or obscene purposes, or in support of such activities;
 - a. Illegal activities shall be defined as a violation of local, state, and/or federal laws.
 - b. Inappropriate use shall be defined as a violation of the intended educational use of the network and/or violation of Board Policy or Administrative Regulation.
 - c. Obscene activities shall be defined as a violation of generally accepted social standards for use of a publicly owned and operated communication vehicle.
2. Intentionally disrupts network traffic, crashes the network and connected systems or damages any equipment;
3. Alters or reconfigures computers, networks, printers or other associated equipment except when directed by the Technology department;
4. Vandalizes equipment or software;
5. Degrades or disrupts equipment or system performance;
6. Uses the CUSD's computers and/or network with the intent of or for commercial or financial gain or fraud;
7. Steals data, equipment, or intellectual property;
8. Gains or seeks to gain unauthorized access to resources or systems, including hacking and using another person's ID and password to access information;
9. Forges electronic documents, including mail messages or uses an account owned by another user;
10. Invades the privacy of individuals
 - a. Accessing another person's materials, information, or files without the implied or direct permission of that person or district management is prohibited;
 - b. Erasing, renaming, modifying, or making unusable anyone else's computer files, programs or media storage devices.
11. Posts anonymous messages except where professionally appropriate;
12. *Using district resources to solicit, create, forward, or reply to any email that could be classified as a chain letter (SPAM).*
13. Creates, distributes, or purposely activates a computer virus;
14. Storage of illegal or inappropriate materials on the system;
15. Uses the CUSD's computers, network, and/or other systems to access, post, submit, publish or display harmful or inappropriate matter that is threatening, obscene, disruptive, sexually explicit, or that could be construed as harassment or disparagement of others based on their race, ethnicity, national origin, sex, gender, sexual orientation, age, disability, religion or political beliefs.;
16. Sends or requests messages or documents that are inconsistent with CUSD or school policies, guidelines, or codes of conduct;
17. Possesses any data that might be considered a violation of these rules in print, or any other form;
18. Bypasses or attempts to bypass any controls put in place on the CUSD's computers or network systems
19. Installs or attempts to install any tool to gain unauthorized access;
20. Installs personal or copyrighted software without appropriate license and approval from the Technology department.

16. Disciplinary Action. Any violation of this Acceptable Use Policy may be cause for restriction or revocation of network access privileges. Said revocation will not inhibit the District's authority to impose disciplinary action as deemed appropriate, up to and including termination. If a staff member is accused of any of the violations listed above, he/she has all of the rights and privileges that a staff member would have if he/she were subject to any other type of disciplinary action.

Signature Required on Next Page

Technology Acceptable Use and Security Policy

PLEASE SIGN BELOW IF YOU AGREE TO THE FOLLOWING STATEMENTS:

- I have read, understand, and agree to the CUSD Acceptable Use Policy. I agree to follow all of the rules contained in this 4-page document. I understand that if I violate the rules, my account can be terminated, my access to computers revoked, and I may face disciplinary measures up to and including termination.
- I understand that Internet sites are filtered and that my District email accounts and Internet use, as well as any other uses of the system or files on the system, may be monitored by the District as described above.
- I hereby release the CUSD, its personnel and any institutions with which it is affiliated, from any and all claims and damages of any nature arising from my use of, or inability to use, the CUSD's network and computer systems, including but not limited to claims that may arise from the unauthorized use of the system.

Staff working with students:

- I agree to enforce the Student Acceptable Use Policy with students under my supervision.

Signature: _____ Date: _____

Printed Name: _____

Current (Anticipated) Work Location _____