Coldspring-Oakhurst CISD
Technology Acceptable Use Policy
(Revised September 2023)

Table of Contents

Technology Staff
Mission and Vision
Availability of Access
Expectations
Inappropriate Use
Email
Social Media Guidelines

- Scope
- Definitions
- School Related Social Media Pages
- Personal Responsibility
- Cyberbullying

Network Behavior
Security
Internet Filter
Internet Safety/Education
District/Department/School/Organization Websites)
Staff Communications
Device Check-out/Check-In
Due Process

Mission and Vision

Mission

The mission of the COCISD Technology Department is to provide the tools, resources and supports that will allow for the effective use and integration of technology in the classroom-learning environment and build the technology literacy and competency of both students and staff.

Vision

Our vision is to provide students and staff access to a network built on a reliable, yet scalable infrastructure that will support the use of current and future technology services.

Availability of Access

COCISD is pleased to offer a wide array of technology resources that include, but are not limited to, use of school technology devices (at school and/or at home), access to a computer network for file sharing, storage, printing, electronic email (email) and the Internet. These services are granted to all students and District employees. The proper use of the technologies provided give students and staff of COCISD the tools needed to integrate technology into classroom instruction, communicate effectively, share resources, collaborate and use 21st Century Skills to achieve technology competency at all levels. The improper, illegal, inappropriate, or unethical use of these technologies can lead to consequences that are harmful to COCISD, its students and its employees. This Acceptable Use Policy as outlined below intends to educate the students and staff of COCISD of the proper use of technology in our district, thus minimizing the likelihood of such harm. Legal Board policies CQ (Local) for Electronic Communication and Data Management and DH (Local) for Employee Standards of Conduct are the basis for these guidelines and any disputes or questions regarding student or staff Acceptable Use of the districts computer systems will be settled at the discretion of COCISD personnel.

Expectations

COCISD expects that all students and staff conduct themselves in a manner that will comply with district guidelines and rules. The COCISD Student Code of Conduct applies to virtual/remote interaction just as it would for face-to-face interaction. Access to the districts electronic communications systems is a privilege, not a right, and may be revoked if abused. Each student and employee is personally responsible for his/her actions when using district technology.

Inappropriate Use

Inappropriate use is considered anything that:

- Violates the law or the guidelines listed in this document
- Causes damage or loss to any property of COCISD
- Poses a security risk to any electronic data or content used by COCISD
- Causes a disruption in the normal functionality of the network
- Interferes with the integrity or security of the COCISD network, or any networks connected to the COCISD network.

Any violations of these guidelines could lead to the loss of your computer/network/internet privileges COCISD. Below are general guidelines to follow to help prevent such loss.

- Do not use district technology to harm another person.
- Do not damage district technology devices or the district network in any way.
- Do not have food or drinks at or near technology equipment.
- Do not take a damaged device to a third party repair shop.
- Do not access, modify, delete or copy another student's work or document
- Do not download, upload, or install any software, programs or malicious content to the network or computers.
- Do not interfere with the operation of the network by accessing or viewing inappropriate material.
- Keep your username and password to yourself.
- Do not save non-educational material, pictures, or music to the devices or the network without permission.
- Do not view, send, or display inappropriate or offensive content.
- Do not use any district electronic communication system(s) in any way that may be considered: (a) Obscene, (b) Offensive, (c) Abusive, (d) Threatening, (e) Harmful to another user, (f) Harassing, (g) Illegal, (h) Pornographic or (i) contrary to district policy.
- Do not attempt to bypass district content filters, or use VPN or proxies, to obtain access to inappropriate or blocked material.
- Do not violate copyright laws.
- Notify a teacher or staff member if you receive or encounter any material that you believe violates the rules of acceptable use.
- Be prepared to be held accountable for your actions and for the loss of privileges if you violate these guidelines or any of the terms of acceptable use.
- Personal laptops, chromebooks, or other electronic devices are NOT allowed at school. COCISD will not assume liability or be held responsible for lost or stolen devices.
- Threatening, or disrespectful language in emails distributed through District email is prohibited.
- Sending messages that could cause danger or disruption, personal attacks, including prejudicial or discriminatory attacks, are prohibited.

- Sending “spam” email or forwarding unsolicited junk mail or chain letters is prohibited.
- Sending “for sale/rent” items via email is prohibited.
- Use of any District electronic system for commercial, income-generating or "for-profit" activities, product advertisement, or political lobbying is prohibited.
- Use of the system for promoting activities or events for individuals or organizations not directly affiliated with or sanctioned by the District is prohibited.

Consequences for inappropriate use can be any of the following:

- Suspension of access to the system and/or network
- Revocation of computer system access; or
- Other disciplinary or legal action, in accordance with the Student Code of Conduct and applicable laws

Email

The use of email at COCISD is for instructional/educational and administrative use only. The sending of jokes, chain emails, political emails, and spam emails, etc. through school email is prohibited and is considered an inappropriate use of COCISD equipment/services. All email and other electronic communications by both staff and students of COCISD are not to be considered confidential and will be archived as digital records for a time period of no less than one year. Email is to be considered a public document and can become part of a legal request through the Public Information Act. When corresponding through any form of electronic communication, always be mindful of the tone, grammar and spelling used. Also, whether intended or not, emails received from your district email account could lead the recipient to think that you are representing the district or school. Email transmissions and other use of technology resources are not confidential and can be monitored at any time to ensure appropriate use.

Social Media Guidelines

SCOPE

This social media policy applies to all COCISD employees, teachers, students, Board Members and auxiliary personnel. This policy covers all social media and media platforms, social networks, blogs, photo sharing, wikis, online forums and video sharing.

Definitions

1. Social Media Account - A personalized presence inside a social networking channel, initiated at will by an individual. YouTube, Twitter, Facebook, Instagram, SnapChat and other social networking channels allow users to sign-up for their own social medial account, which they can use to collaborate, interact and share content and status updated. When a user communicates through a social media account, their disclosures are attributed to their User Profile.
2. Social Media Channels - Blogs, micro-blogs, wikis, social networks, social bookmarking services, user rating services and any other online collaboration, sharing or publishing platform, whether accessed through the web, a mobile device, text messaging, email or other existing or emerging communications platforms.
3. Hosted Content - Text, pictures, audio, video or other information in digital form that is uploaded and resides in the social media account of the author of a social media disclosure. If you download content off the Internet, and then upload it to your social

media account, you are hosting that content. This distinction is important because it is generally illegal to host copyrighted content publicly on the Internet without first obtaining the permission of the copyright owner.

4. Copyrights - Copyrights protect the right of an author to control the reproduction and use of any creative expression that has been fixed in tangible form, such as literary works, graphical works, photographic works, audiovisual works, electronic works and musical works. It is illegal to reproduce and use copyrighted content publicly on the Internet without first obtaining the permission of the copyright owner.
5. Official Content - Publicly available online content created and made public by Coldspring-Oakhurst CISD.
6. Blog - An online journal that contains entries or posts that consist of text, links, images, video or other media and is usually between 300-500 words.
7. Microblogging - n: Posting brief and often frequent updates online. Unlike traditional blogs, which are often hosted on a custom website, microblogs are typically published on social media sites like Twitter, Instagram, Tumblr and Facebook.
8. Cyberbully - Cyberbullying is the use of electronic information and communication devices, to include, but not limited to, email messages, instant messaging, text messaging, cellular telephone communications, Internet blogs, Internet chat rooms, Internet postings and defamatory websites.

School-Related Social Media Pages

- **Any Social Media Page that represents a COCISD school, department, club or organization must have district approval from PR Coordinator prior to creation.**

Personal Responsibility

Faculty and Staff

- COCISD employees are personally responsible for the hosted content they publish online. Be mindful of what you post on social media channels.
- When posting online, please remember that you are an employee of COCISD and a representative of your colleagues, students, parents and the school community.
- Your online behavior should reflect the same standards of honesty, respect and consideration that you use face-to-face.
- Do not post photos or movies of fellow employees without their permission. Do not use photos or movies taken at school without permission. Do not post photos or movies that contain students without parental consent.
- Many websites allow users to share personally created movies. You are responsible for all you do, say and post online including videos. Anything posted online should represent you in a professional manner, as others will see you as connected to COCISD.
- When posting online be sure not to post confidential student information.

Students

- I will not give my home address, location of my school, phone number or any personal information about myself or any other student or school personnel to anyone via the Internet.
- COCISD students are personally responsible for the hosted content they publish online. Be mindful of what you post on social media channels.
- Cyberbullying is not to be tolerated, and is to be taken seriously. Any incidence of cyberbullying should be reported to the school Principal immediately.
- Do not post photos or movies of fellow students without their permission. Do not use photos or movies taken at school without permission.

- Many websites allow users to share personally created movies. You are responsible for all you do, say and post online including videos.

Personal use of social networking site, including Facebook, Twitter and Instagram

- COCISD employees are not permitted to solicit or accept "Friend" Requests from enrolled COCISD students on any personal Social Media Account. This includes student's accounts and COCISD employee personal accounts.
- COCISD staff and employees are personally responsible for all comments/information and hosted content they publish online. Be mindful that things such as Tweets and Status Updates will be visible and public for a long time.
- By posting comments, having online conversations, etc. on social media sites you are broadcasting to the world. Be aware that even with the strictest privacy settings, what you 'say' online should be within the bounds of professional discretion. Comments expressed via social networking pages under the impression of a 'private conversation' may still end up being shared into a more public domain, even with privacy settings on maximum.
- Comments related to COCISD, its employees, staff and/events related to COCISD, should always meet the highest standards of professional discretion. When posting, even on the strictest settings, staff should act on the assumption that all postings are in the public domain.
- Before posting photographs and videos, permission should be sought from the subject where possible. This is especially the case where photographs of professional colleagues are concerned.
- Photographs relating to alcohol or tobacco use may be deemed inappropriate. Remember, your social networking site is an extension of your personality, and an extension of your professional life and classroom. If it would seem inappropriate to put a certain photograph on the classroom wall, then it should be considered inappropriate to post online.
- Microblogging (Twitter, Facebook, Tumblr, Instagram, etc.) comments made using such media are not protected by privacy settings. Employees should be aware of the public and widespread nature of such media and refrain from any comment and/or #hashtags that could be deemed unprofessional.

Cyberbullying

Cyberbullying by a COCISD student or school staff member directed toward another COCISD student or school staff member is conduct that disrupts both a pupil's ability to learn and a school's ability to educate its pupils in a safe environment.

COCISD prohibits acts of cyberbullying by COCISD students and staff members through the use of any COCISD owned, operated, and supervised technologies. The school principal or designee may report allegations of cyberbullying to law enforcement authorities.

Any act online, or through electronic devices (cellular phones, tablets) that deliberately threatens, harasses, intimidates an individual or group of individuals; places an individual in reasonable fear of harm to the individual or damage to the individual's property; has the effect of substantially disrupting the orderly operation of the school is considered cyberbullying.

Any student or school staff member who believes he/she has, or is being subjected to, cyberbullying, as well as any person who has reason to believe a student or school staff member has knowledge or reason to believe another pupil or school staff member is being

subjected to, or has been subjected to, cyberbullying shall immediately make a report to the school principal or designee.

COCISD has a zero tolerance policy against cyberbullying and each reported instance will be handled in accordance with district, local and state rules, policies and guidelines.

Network Behavior

COCISD students and staff members will be given network accounts that will allow access to the District computers, network and any resources allowed by permissions granted. Each user will be held responsible for their actions while accessing available resources. The following are guidelines that will apply to all users:

- Each user will always be responsible for the proper use of their account. At no point should a user share his/her account information to give another user access to the network.
- District Employees will be required to maintain a password for their account and should always keep that password confidential. In some cases, the user may be required to change their password on a regular schedule.
- District users should not install or alter any programs or software on the network. Any unauthorized installation of software onto network servers, classroom/library computers or any other electronic device is prohibited.
- The network should not be used in a manner that is thought to be illegal, offensive, a security risk or in violation of any other act prohibited by District policy.

Security

COCISD will make every attempt to keep the network and computers secure from malicious software, viruses, malware, and attempted hacks. If a user of District network resources has knowledge of a possible security risk, the user should immediately notify district technology staff or the campus administrator. Any attempt by district users to load malicious software, viruses, malware, or hack into unauthorized District resources will be treated as a violation of these guidelines and be subject to loss of privileges or other consequences. Below are guidelines to help maintain security and integrity of the district network and its resources:

- At no point should a student work on computer workstation using a teacher or staff member's login.
- Staff members should not allow students on their classroom workstations unless the user is logged in under his/her name and is closely monitored by the teacher.
- Teachers and students should make every attempt to keep their computer secure when logged in by either locking the workstation or protecting it with a password protected screensaver.
- At no point should a student or unauthorized staff member be allowed to work in any District or campus program that is used for maintaining student/employee records, administrative/budgetary documentation.

Internet Filter

As required by the Children's Internet Protection Act (CIPA), the district maintains a filtering system that blocks access to information considered obscene, pornographic, inappropriate for students or harmful to minors as defined by the federal CIPA guidelines. Families should be aware that even with our filters in place, some material accessed on the Internet may

still contain inappropriate content. While the purpose of the district is to use the Internet and other resources for constructive educational goals, students may find ways to gain access to other materials. Any attempt to gain access to sites not allowed by our Internet content filters will be deemed inappropriate use and could lead to loss of privileges or other consequences. Your agreement to this policy also acknowledges that you give consent for your child to have access to YouTube for various instructional assignments. The district shall not be liable for users' inappropriate use of district technology equipment or resources, violations of copyright restrictions or other laws, users' mistakes or negligence, and/or costs incurred by the users.

Internet Safety/Education

It is every staff member's responsibility to educate students about appropriate online behavior, including interactions with other individuals on social networking sites/chat rooms, and cyber bullying awareness and response. In compliance with the Children's Internet Protection Act (CIPA) and as required by Legal Board Policy CQ (Legal), COCISD will develop and follow an Internet Safety plan that will protect and educate the students and staff of COCISD. The following procedures and guidelines are in place at COCISD:

- Minor access to inappropriate and harmful materials will be controlled and monitored using District content filters.
- Email use by students will be closely monitored by the district content filter and District Staff.
- Students and staff will be educated in only using their login credentials to gain access to District resources. At no time should someone else's login credentials be used.
- All information and data pertaining to students will be protected and used in a responsible manner as so not to allow unauthorized access, use, or dissemination.
- COCISD will educate minors about appropriate online behavior, including interacting with other individuals on social networking websites in chat rooms and cyber bullying awareness. The following steps are in place to ensure compliance:
    - COCISD uses videos and lessons from Kidsmartz.org and Learning.com to educate students about cyber safety, online conduct, real world situations, and cyber bullying.
    - COCISD uses grade-appropriate videos and lesson plans for grades 6-12 from various sources to educate students about cyber safety, online conduct, and cyber bullying. These lessons are assigned by the District Instructional Technology Specialist to ensure that every student is educated in this area.

District/Department/School/Organization Websites

Overview

COCISD has and maintains an official website that will provide individuals with information about the District. Contained within the district website are campus websites, teacher websites, department websites, and organization websites. Websites at all levels should follow these guidelines to ensure that they represent COCISD in a professional manner:

- All web pages should be checked for spelling, grammar, and professionalism.
- All copyright laws for publications shall be followed.
- All pages should be kept up-to-date.

- All pages linked to your district web page should be checked for content and appropriateness.
- If you maintain an external website, blog or wiki, it should be linked to your district-provided website.

Schools and administrative departments may publish names, photos, and individual work of students or staff on web pages to recognize achievements and awards if the appropriate permission slips are on file in the office. Please ensure that these permission slips are up to date and for the current school year.

Staff Communications

All staff members are expected to comply with Senate Bill 944:
SENATE BILL 944 makes government employees (school staff) TEMPORARY CUSTODIANS OF PUBLIC INFORMATION Effective date: September 1, 2019.
Temporary Custodians: This bill adds a new definition in the Public Information Act (PIA) for a temporary custodian to mean a former or current employee or officer of a governmental body who, in the transaction of official business, creates or receives public information that has not been provided to the governmental body's public information officer (PIO). In a school district, the superintendent is the PIO. Information held by a temporary custodian is subject to records preservation, retention, and disposition requirements under Texas Government Code. A temporary custodian must surrender or return information in his or her possession within 10 days of a request from the PIO or PIO's agent. Failure to comply is grounds for disciplinary action if employed by the governmental body, and subject to any applicable penalties under the PIA or other law. Information on Personal Devices: This bill provides that a current or former employee or officer of a governmental body has no personal or property right to public information created or received while acting in an official capacity. The bill requires all current and former officers and employees of a governmental body who maintain public information on a privately owned device to either: (1) forward or transfer the public information to the governmental body or the body's server to be preserved for the legally requisite retention periods; or (2) preserve the information in its original form in a backup or archive on the privately-owned device for the legally requisite retention periods.
COCISD will utilize District-provided accounts to store all correspondence and communication related to school business between students and staff, parents and staff, and work-related communication between staff members. These accounts include the District Remind application, District-provided email accounts, and other District applications such as Google Classroom.
Staff members should never text students from their personal cell phones, or instant message/direct message students on any social media, messaging app or account. All communication needs to take place via Remind, school email, or other District-provided academic applications such as Google Classroom. No communication that could be considered PIA information should be deleted.

Device Check-out/Check-In

Overview

The District has iclassroom carts with mobile devices (Chromebooks, iPads, etc.) for student use. Student use is encouraged and expected when

appropriate within the curriculum and lesson being taught. As important as these devices are to student achievement, proper check-out/check-in procedures and monitoring by staff, as well as appropriate use by students, will be expected. To ensure these devices remain functional and usable, the following expectations for students and staff should be adhered to.

Expectations

- Each student will be assigned to a specific device in their class for use each day.
- Staff should routinely (once a week) inspect all devices in their classroom and document any problems that are found.
- Devices must be returned to the cart at the end of each class period.
- Students will only use the device that has been assigned to them.
- Students will only remove devices from carts under the teacher's supervision.
- If the device is broken or is not working properly, the student should report the problem immediately to the teacher who should then report it to Technology Dept.
- Students should always use the device for its intended use and within the guidelines outlined in this document.
- Classroom devices are not to be used by students when there is a substitute teacher in the classroom. The classroom teacher will be responsible for leaving assignments to the substitute that do not require the use of classroom technology devices by the students.

Due Process

In the event there is a claim that you have violated district policy in your use of the system, you will be provided with a written notice of the suspected violation and an opportunity to present an explanation before an administrator in the manner set forth by district policy. Noncompliance may result in suspension of access or termination of privileges and other disciplinary action consistent with district policies. The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's electronic communications system.

Acceptance of these Guidelines:

Parent Permission Form and Student Agreement

As a parent or guardian of a student attending COCISD, I have read the above information regarding the appropriate and acceptable use of computers and I understand that this agreement will be on file at the school.

☐ Yes, I do give my child permission to utilize the Electronic Data Communication System provided by COCISD and agree to the policy and guidelines for acceptable use.

☐ No, I do not give my child permission to utilize the Electronic Data Communication System provided by COCISD.

Parent Name (Print) _____

Date _____

As a student attending COCISD, I have read the above information regarding the appropriate and acceptable use of the districts computers and network and I agree to comply with the guidelines and to use the computers and network in constructive manner.

Student Name (Print) _____

Student Signature _____

This agreement is perpetual and remains in effect indefinitely, but can be revoked by written authorization from the parent/guardian.

Staff Agreement to Acceptable Use Guidelines

As an employee of COCISD, I have read the above information regarding the appropriate and acceptable use of the districts computers and network and I agree to comply with the guidelines and to use the computers and network in a constructive manner.

Employee Name (Print) _____

Employee Signature _____