SCOPE

The Superintendent or designee will oversee the District's electronic communications system. The District will provide training in proper use of the system and will provide all users with copies of acceptable use guidelines. All training in the use of the District's system will emphasize the ethical and safe use of this resource.

CONSENT REQUIREMENTS

Copyrighted software or data may not be placed on any system connected to the District's system without permission from the holder of the copyright. Only the copyright owner(s) or individual(s) the owner specifically authorizes may upload copyrighted material to the system. No original work created by any District student or employee will be posted on a Web page under the District's control unless the District has received written consent from the student (and the student's parent if the student is a minor) or employee who created the work). No personally identifiable information about a District student will be posted on a Web page under the District's control unless the District has received written consent from the student's parent. An exception may be made for information as allowed by the Family Educational Rights and Privacy Act and District policy.

CHIEF TECHNOLOGY OFFICER RESPONSIBILITIES

The Chief Technology Officer for the District's electronic system will:

1. Be responsible for disseminating and enforcing applicable District policies and acceptable use guidelines for the District's systems.

2. Ensure that all users of the District's system annually sign an agreement to abide by District policies and administrative regulations regarding such use. All such agreements will be maintained on file in the principal's or supervisor's office.

3. Ensure that employees supervising students who use the District's system provide training emphasizing the appropriate use of this resource.

4. Ensure that all software loaded on computers in the District is consistent with District standards and is properly licensed.

5. Be authorized to monitor or examine all system activities, including electronic mail transmission, as deemed appropriate to ensure student safety online and proper use of the system.

6. Be authorized to disable a filtering device on the system for bona fide research or another lawful purpose, with approval from the Superintendent or designee.

7. Be authorized to establish a retention schedule for messages on any electronic bulletin board and to remove messages posted locally that are deemed to be inappropriate.

8. Set limits for data storage within the District's system, as needed.

SYSTEM ACCESS

Access to the District's electronic communications system will be governed as follows:

1. As appropriate and with the written approval of the immediate supervisor, District employees will be granted access to the District's system.

2. As appropriate and with the written approval of the Superintendent or designee, non-employees will be granted access to the District's system.

3. Students will be granted access to the District's system by their teachers, as appropriate. Students will be assigned individual accounts as appropriate.

4. The District requires that all passwords be changed every 90 days.

5. Any system user identified as a security risk or as having violated District and/or campus computer user guidelines may be denied access to the District's system.

6. Violation of any of the procedures outlined in policy or this regulation will result in cancellation of system use privileges and will require restitution for costs associated with system restoration, as well as other appropriate disciplinary consequences including termination, student expulsion, or filing of criminal charges. [See DH, FN series, FO series, and the Student Code of Conduct]

7. All users will be required to sign a user agreement annually for issuance or renewal of an account.

INDIVIDUAL USER RESPONSIBILITIES ON-LINE CONDUCT

The following standards will apply to all users of the District's electronic information/communications systems:

1. The individual in whose name a system account is issued will be responsible at all times for its proper use.
2. The system shall not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District Policy, Regulations, and guidelines.
3. The system shall not be used for personal profit or for political purposes.
4. System users shall not disable, or attempt to disable, a filtering device on the District's electronic communications system.
5. Communications shall not be encrypted so as to avoid security review by system administrators.
6. System users shall not use another person's system account without written permission from the campus administrator or Chief Technology Officer, as appropriate.
7. Students shall not distribute personal information about themselves or others by means of the electronic communication system; this includes, but is not limited to, personal addresses and telephone numbers. High school students are exempt from this guideline only while completing online registrations in association with the campus Counseling Center regarding college entrance exams, college and career planning, and college applications.
8. Students shall not make appointments to meet people whom they meet on-line and must report to a teacher or administrator if they receive any request for such a meeting.
9. System users must purge electronic mail in accordance with established retention guidelines.
10. System users shall not redistribute copyrighted programs or data except with the written permission of the copyright holder or designee. Such permission must be specified in the document or must be obtained directly from the copyright holder or designee in accordance with

applicable copyright laws, District policy, and administrative regulations.

11. System users must obtain written approval from the Chief Technology Officer or designee for permission to install software not purchased by the District onto any District computer. Only designated technology personnel may install or download software on District computers.
12. System users shall not send or post messages that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, or damaging to another's reputation or illegal.
13. System users shall not purposefully access materials that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation or illegal.
14. System users shall not purposefully proxy a computer outside the District to access materials or commit actions that are in violation of District Policy, Regulations, and guidelines.
15. System users should be mindful that use of school-related electronic mail addresses might cause some recipients or other readers of that mail to assume they represent the District or school, whether or not that was the user's intention.
16. System users shall not waste District resources related to the electronic communications system.
17. System users shall not gain unauthorized access to resources or information.

VANDALISM PROHIBITED

Any malicious attempt to harm or destroy District equipment or data of another user of the District's system or of any of the agencies or other networks that are connected to the Internet is prohibited. Deliberate attempts to degrade or disrupt system performance are violations of District policy and administrative regulations and may constitute criminal activity under applicable state and federal laws. Such prohibited activity includes, but is not limited to the uploading or creating of computer viruses. Vandalism as defined above will result in the cancellation of system use privileges and will require restitution for costs associated with system restoration, as well as other appropriate consequences.

FORGERY PROHIBITED

Forgery or attempted forgery of electronic mail messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other system users, deliberate interference

with the ability of other system users to send/receive electronic mail, or the use of another person's ID and/or password is prohibited.

INFORMATION CONTENT THIRD-PARTY SUPPLIED INFORMATION	System users and parents of students with access to the District's system should be aware that, despite the District' use of technology protection measures as required by law, use of the system may provide access to other electronic communications systems in the global electronic network that may contain inaccurate and/or objectionable material. A student who gains access to such material is expected to discontinue the access as quickly as possible and to report the incident to the supervising teacher. A student knowingly bringing prohibited materials into the school's electronic environment will be subject to suspension of access and/ or revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the Student Code of Conduct. An employee knowingly bringing prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with District policies. [See DH]
PARTICIPATION IN CHAT ROOMS AND NEWSGROUPS	Participation in chat rooms and newsgroups accessed on the Internet is permissible for employees and students, under appropriate supervision, for educational purposes only.
DISTRICT WEB SITE	The District will maintain a District Web site for the purpose of informing employees, students, parents, and members of the community of District programs, policies, and practices. Requests for publication of information on the District Web site must be directed to the Office of Communications. The Chief Technology Officer and Office of Communications establish guidelines for the development and format of Web pages controlled by the District. No personally identifiable information regarding a student will be published on a Web site controlled by the District without written permission from the student's parent.
PERSONAL USE OF ELECTRONIC MEDIA	Employees in a public school system are responsible for modeling and teaching high standards of decency and civic values. District employees must model the character they are expected to teach, both on and off the worksite. This applies to material posted on personal websites and other internet sites, such as MySpace or Facebook. Messages or pictures that diminish the employee's professionalism impair the employee's ability to maintain the respect of students and parents and impede the employee's ability to effectively perform his or her job. This type of material includes, but is not limited to, text or

pictures involving hate speech, nudity, obscenity, vulgarity, conduct illegal for a minor, or sexually explicit content. Posting such materials may be grounds for termination or other disciplinary action.

Employees who maintain private social networking sites for their private use shall not share that site with students.

Employees are encouraged to utilize the communication tools and technology resources available through the District, including the learning management system. Employees who act as sponsors for teams or clubs who wish to establish an outside website or social networking site to communicate with members shall have principal approval in addition to obtaining written parental permission from each student "invited" to the site. The site must also meet CCISD Technology security requirements, if used on the CCISD network and be approved by the technology department. Both the parent and student must be given access to the site. Permission slips must be maintained in accordance with the District's records retention schedule. In addition, the site should be kept private so that only school officials and specific students and their parents have access.

The employee may not set up or update the employee's personal social network page(s) using the district's computers, network, or equipment.

PERSONAL WEB PAGES

District employees, Trustees, students and members of the public will not be permitted to publish personal Web pages using District resources.

EMAIL RETENTION

It is the responsibility of the user to manage e-mail messages according to the District's records retention schedule. Names of the sender, recipient, date/time of the message, as well as any attachments, must be retained with the message. Electronic mail communication systems are used to facilitate daily communications and are not intended as an archival storehouse for non-current communications. Electronic mail messages generally should be deleted upon review of the communications, and, absent limited exceptions, should not be maintained beyond 90 days. In accordance with the District's information retention policy, information contained in e-mail communications may be retained for longer terms in a number of formats, including in separate electronic formats and on paper. Questions regarding the retention requirements applicable to particular types of information should be referred to the District's records retention department. Retention

Periods: The District complies with state requirements governing records retention. The complete records retention schedule can be found on the Internet at: http://www.tsl.state.tx.us/slrm/recordspubs/sd.html. Users are advised to consult this schedule for the retention period applicable to the information they use or create in the course and scope of performing job functions.

EMAIL PERSONAL USE

All CCISD resources owned or paid for by the district are the property of CCISD and are made available to users for the purpose of conducting district business. Users may not perform any personal or non-work activities, except for incidental personal activities that comply with all CCISD policies, specifically Policy CQ Local. Incidental personal activities refer to short term use that does not interfere with a user's normal work activities, such as making a personal phone call that lasts a few minutes. CCISD may, at its sole discretion, limit or restrict any user's personal usage of or access to electronic resources. The district also reserves the right to remove unauthorized content from such resources without advance notice. To help assess the appropriateness of your use of district resources, consider whether your supervisor would share your judgment that your use is for business or educational purposes.

EMAIL OWNERSHIP

All email accounts maintained on our email systems are the property of CCISD. The district owns any communication sent via email or that is stored on district equipment. Management and other authorized staff have the right to access any material in your email or on your computer at any time.

No expectation of privacy exists in anything you create, store, send or receive on the district's systems. Your emails can be monitored without prior notification if the district deems it necessary and may be subject to disclosure to third parties pursuant to a request under the Texas Public Information Act. Failure to adhere to the guidelines set forth in the policy and regulation may result in disciplinary action up to and including termination.

EMAIL GENERAL USAGE

CCISD users must use extreme caution when opening email attachments received from both known and unknown senders as these may contain viruses, email bombs or Trojan horse code. Use extra care if the email contains a link or attachment that has a file extension you are not familiar with. If a user does open an attachment and releases malicious code, s/he must remove the computer from the network immediately and report the incident to the IT Help Desk.

Users should at no time respond to a message requesting their user id, password or personal information. Emails may appear to be from a well-known organization; however, users should never share CCISD related account or password information.

Users should log out of their mailboxes or lock their computers when they are going to be away.

Users will not be permitted to create personal archives (or "PSTs") on individual hard drives, shared drives or other devices to store emails.

EMAIL / MAILBOX LIMITS

The following usage limits have been established for mailboxes and messages

Messages sent internally will be limited to 20 MB per message
Messages sent externally or received from external sources will be limited to a size of 20 MB per message
A warning message will be sent when the Mailbox size limit reaches 90% capacity.
Users will be prohibited to send email messages if the Mailbox size limit reaches 90% capacity.
Emails older than 2 years will be purged from the system.

APPROVED MOBILE DEVICES

CCISD only supports district owned mobile devices for access to email system. Passwords on the devices will be enabled and the device will be locked after 15 minutes. Access to district email will no longer be available upon separation from the district.

Employees may access district email from personally owned devices. However, be aware that all policies related to access to CCISD systems still apply. The CCISD Help Desk will not support personal mobile devices, however information can be found on the employee portal if you would like to set up your device.

BEST PRACTICES

CCISD considers email to be an important means of communication and expects users to adhere to the following guidelines:

1. Write well-structured emails and use short, descriptive subjects.
2. Signatures must include your name, job title, department or school and district name.
3. Use the spell check before you send out an email.

4. Do not send unnecessary attachments. Compress attachments larger than 200k before sending them.
5. Do not write emails in capitals.
6. Do not use cc: or bcc: fields unless the cc: or bcc: recipient is aware that you will be copying an e-mail to him/her and knows what action, if any, to take.
7. If you forward emails, state clearly what action you expect the recipient to take.
8. Only send emails of which the content could be displayed on a public notice board. If they cannot be displayed publicly in their current state, consider rephrasing the email, using other means of communication, or protecting information by using a password.
9. Only mark emails as important if they really are important.

For system functionality purposes and in order to reduce the cost of storing, indexing, and handling the vast amounts of email generated and received by users on a daily basis, users should routinely delete all emails that have no ongoing educational, business, operational, referential or legal value, and that are not otherwise subject to retention. Thus, all drafts, notes, routine communications and the like, shall be routinely destroyed immediately after they no longer have any value. See EMAIL RETENTION above.

Delete any email messages that you do not need to retain, and set your email client to automatically empty your 'deleted items' on closing.

TRANSFER OF EQUIPMENT TO STUDENTS

The following rules will apply to all campuses and departments regarding transfer of computer equipment to students under provisions of law cited at CQ (LEGAL):

1. Proposed plans to distribute computer equipment to students must be submitted to the Chief Technology Officer for initial approval.
2. A student is eligible to receive computer equipment under these rules only if the student does not otherwise have home access to equivalent equipment at home, as determined by the principal and campus technology staff, or assistive technology staff, as appropriate.
3. In transferring computer equipment to students, preference will be given to educationally disadvantaged students.
4. Before transferring computer equipment to a student, the principal and campus technology staff, or assistive technology staff must have clearly documented, and approved by the Chief Technology Officer:

a. A process to determine eligibility of students;
b. An application process that identifies the responsibility of the student regarding home placement, use, and ownership of the equipment;
c. A process to distribute and initially train students in the setup and care of the equipment;
d. A process to provide ongoing technical assistance for students using the equipment;
e. A process to determine the need for ongoing student use of the equipment;
f. A process to determine the impact on student achievement the use of this equipment may provide;
g. A process for return of the equipment from a student; and
h. A process for retrieval of the equipment from a student, as necessary.

TERMINATION/ REVOCATION OF SYSTEM USER ACCOUNT

Termination of an employee's or student's access for violation of District policies or regulations will be effective on the date the principal or Chief Technology Officer or designee receives notice of employee termination, student withdrawal or of revocation of system privileges, or on a future date if so specified in the notice.

DISCLAIMER

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether expressed or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District does not warrant that the functions or services performed by, or that the information or software contained on the system will meet the system user's requirements, or that the system will be uninterrupted or error free, or that defects will be corrected. Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third-party individuals in the system are those of the providers and not the District. 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.