Note: For information regarding use of the District's technology resources and electronic communications by Board members, see BBI(LOCAL). For student use of personal electronic devices, see FNCE. For additional provisions governing employee use of electronic media, see DH(LOCAL) and the District's employee handbook. For information regarding retention and security of records containing criminal history record information, as well as procedures for reporting security incidents regarding such information, see DBAA. For information regarding District, campus, and classroom websites, see CQA. For information regarding intellectual property and copyright compliance, see CY. For information regarding the District's cybersecurity plan, see CQB.

Scope

The Superintendent or designee will oversee the District's electronic communications system.

Available Technology Resources

The District makes technology resources available to staff, students, parents, and members of the public as applicable and in accordance with the District's conditions of use. Available technology resources may include onsite internet access, District-owned hardware and software, District-approved online educational applications for use at school and at home, and digital instructional materials.

Internet Safety Plan

The Superintendent will designate the Chief Technology Officer to oversee development and implementation of an internet safety plan, including guidelines for the acceptable use of the District's technology resources in compliance with this plan. All users will be provided copies of acceptable-use guidelines and training in proper use of the District's technology resources that emphasizes ethical and safe use. [EXHIBITS A & B].

Filtering

The Superintendent will appoint a committee, to be chaired by the technology coordinator, to determine appropriate use of filtering devices. The Superintendent will designate the Chief Technology Officer to implement and maintain appropriate technology for filtering material considered inappropriate or harmful to minors. All internet access will be filtered for minors and adults on the District's network and computers with internet access provided by the school.

The categories of material considered inappropriate and to which access will be blocked will include, but not be limited to, nudity or pornography; images or descriptions of sexual acts; promotion of violence, illegal use of weapons or drugs, discrimination, or

participation in hate groups; instructions for performing criminal acts (e.g., bomb making); and online gambling.

Requests to Disable Filter

The committee will consider requests from users who wish to use a blocked site for bona fide research or other lawful purposes. The committee will make a recommendation to the Superintendent regarding approval or disapproval of disabling the filter for the requested use.

System Access

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

General Guidelines

1. All students, employees, and Board members will be provided access to relevant policies and information concerning use of District technology resources and the District's expectations for acceptable use.
2. All students, employees, and Board members will be required to complete training regarding safe and appropriate use of the District's technology resources, including cyberbullying awareness and response, data security, and cybersecurity measures. [See CQB]
3. All district technology resource users will be required to sign a responsible-use agreement annually for issuance of an account.
4. As appropriate and with the written approval of the immediate supervisor, District employees will be granted access to the District's system.
5. As appropriate and with the written approval of the Superintendent or designee, non-employees will be granted access to the District's system. All nonschool users, including volunteers and contractors, will be required to sign or accept a responsible-use agreement annually. Access may be limited by the District as appropriate. [See CQ(EXHIBIT C]]
6. Students will be granted access to the District' s system as appropriate. Students will be assigned individual accounts as appropriate.
7. All passwords for District accounts must meet password complexity requirements established by the District. Passwords must be changed every 90-120 days. All passwords must remain confidential and should not be shared.
8. Any user identified as a security risk or as having violated District and/or campus-use guidelines may be denied access to the District's technology resources.

Board Members and All District Employees

1. With written approval of the immediate supervisor or the Superintendent, and upon completion of District network training, District employees and Board members will be granted access to the District's technology resources, as appropriate. [See BBI]
2. Before use in the classroom, use with students, or administrative use, all digital subscriptions, online learning resources, online or mobile applications, or any other program requiring the user to accept terms of service or a user agreement, or that requires the user to share confidential or individually identifiable information, must be approved by the Chief Technology Officer. District staff and Board members should not accept terms and conditions or sign user agreements on behalf of the District without approval.
3. Teachers and other professional staff must submit a request to use additional online technology resources that have not been approved by the District, as described below at Approval of Technology Resources.
4. Continued use of District technology resources is conditioned on completion of all required training and compliance with all policies and directives regarding use. Failure to complete required training by applicable deadlines will result in immediate suspension of network access and/or device functions and will require reauthorization from a supervisor.
5. The individual in whose name a system account is issued will be responsible at all times for its proper use.
6. 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.
7. The system shall not be used for personal profit or for political purposes.
8. System users shall not disable, or attempt to disable, a filtering device on the District's electronic communications system.
9. Communications shall not be encrypted, unless authorized by the Chief Technology Officer, so as to avoid security review by system administrators.
10. System users shall not use another person's system account without written permission from the campus administrator or Chief Technology Officer, as appropriate.

11. 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.

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.

Instructional Staff

1. Students may only be assigned to use resources approved by the District. To view the most updated list of approved resources, go to the District's website.

2. Parental consent must be obtained before a student may take part in District-sponsored technology, social media, online educational programs or mobile applications, or other cloud-based instructional resources, including video sharing for classroom use or use of a student's photo, image, or voice on a District or classroom website, even if public access is blocked.

3. The staff member assigning students to use technology resources is responsible for ensuring parents and/or students have signed the District's acceptable use agreement and that students have received any required technology training.

4. Management of student use of technology is the responsibility of the staff member in the same manner as classroom management or student supervision.

5. Staff may only record or allow recording of a student's image or voice for the limited purpose of instruction, in compliance with law, policy and administrative regulations. [See EHA, FL, FM, and FO]

6. Disclosure of student directory information for limited school-sponsored purposes may be authorized only in accordance District policy and requisite parent notice and consent. [See FL]

Students

1. Students will be granted access to the District's technology resources as determined by the campus principal.

2. Students under the age of 13 (generally students in pre-kindergarten–grade 7) will have access to District-managed online educational applications and will not be issued or asked to create individual accounts using personally identifiable information.

3. Students may have access to District-issued email or network accounts only as approved by the campus principal and only with parental permission.

4. With parental approval, students will be assigned individual accounts and passwords for use of District-sponsored technology resources, including individual email accounts and District-approved online educational resources.

5. Students granted access to the District's technology resources must complete any applicable user training, including training on cyberbullying awareness and response, copyright piracy, cybersecurity, and appropriate online behavior and interactions with other individuals on social media networking websites.

6. Parental notice and approval will be required before a student may take part in District-sponsored social media, online instructional programs, or other online or mobile educational applications, including video sharing for classroom use or use of a student's photo on a District or classroom website, even if public access is blocked.

7. Upon request from a parent, the District will provide a list of technology resources for use by the student.

Nonschool Users

1. Nonschool users may be given limited access to District technology resources when available, including computer and internet access, online job applications, and access to the District's wireless internet, in accordance with guidelines established by the campus or the District.

2. Use of District technology resources by members of the public may not interrupt instructional activities or burden the District's network.

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 may result in the cancellation of system use privileges and may 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's 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 Board Policy DH]

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 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 Website controlled by the District without written permission from the student's parent.

Communicating with Students Through Electronic Media

A certified or licensed employee, or any other employee designated in writing by the superintendent or a campus principal, may communicate through District-approved electronic media with students who are currently enrolled in the district. The employee must comply with the provisions outlined below. All other employees are prohibited from communicating with students who are enrolled in the district through electronic media. An employee is not subject to these provisions to the extent the employee has a social or family relationship with a student. For example, an employee may have a relationship with a niece or nephew, a student who is the child of an adult friend, a student who is a friend of the employee's child, or a member or participant in the same civic, social, recreational, or religious organization. An employee who claims an exception based on a social relationship shall obtain and provide, upon District request, written consent from the student's parent acknowledging that the parent is aware of the relationship and that the electronic communication falls outside the parameters of the employee's duties with CCISD. [See Board Policy DH]

Electronic media includes all forms of social media, including but not limited to text messaging, instant messaging, electronic mail (e-mail), Web logs (blogs), electronic forums (chat rooms), video-sharing Web sites (e.g., YouTube), editorial comments posted on the Internet, social network sites, and applications. (e.g., Facebook, Twitter, LinkedIn, Instagram, Snapchat, Kik, etc.). Electronic media also includes all forms of telecommunication such as landlines, cell phones, and Web-based applications. [See Board Policy DH]

Communicate means to convey information and includes a one-way communication as well as a dialogue between two or more people. A public communication by an employee that is not targeted at students (e.g., a posting on the employee's personal social network page or a blog) is not a communication: however, the employee may be subject to district regulations on personal electronic communications. See Personal Use of Electronic Media, below. Unsolicited contact from a student through electronic means is not a communication.

An employee who is permitted to use electronic media to communicate with students shall observe the following shall limit all electronic communication to matters within the scope of the employee's professional responsibilities (e.g., for classroom teachers, matters relating to class work, homework, and tests; for an employee with an extracurricular duty, matters relating to the extracurricular activity).

The employee is prohibited from knowingly communicating with students through a personal social network page or site; the employee may create a separate social network page ("professional page") for the purpose of communicating with students, but must obtain prior written principal approval. The employee must enable administration and parents to access the employee's professional page, and private messaging on such pages is prohibited.

Text messaging with students is generally NOT permitted. Only an employee or contracted worker who has a cocurricular or extracurricular duty may use text messaging as part of an approved activity, and then only to communicate with students who participate in the cocurricular or extracurricular activity over which the employee has responsibility regarding that activity. Prior to communicating with students via text messaging, the employee must obtain written approval from the campus principal on CQ(EXHIBIT D) **AND** must obtain written permission from the parent/guardian of each student on CQ(EXHIBIT E). **In addition**, the employee must follow one, more or all of the following procedures, as specifically required by the campus principal:

1. The employee may only text message with students using a specific group messaging application approved by the principal.
2. The employee must include the student's parent as a recipient on all text messages.
3. The employee must include his or her immediate supervisor or designee as a recipient on all text messages.
4. The employee must send a copy of the text message to the employee's district email address.

Personal Use of Electronic Media

The employee does not have a right to privacy with respect to communications with students and parents.

The employee continues to be subject to applicable state and federal laws, local policies, administrative regulations, and the Texas Educators' Code of Ethics, including: (1) compliance with the Public Information Act and the Family Educational Rights and Privacy Act (FERPA), including retention and confidentiality of student records. [See CPC and FL]; (2) copyright law [See Board Policy CY]; and (3) prohibitions against soliciting or engaging in sexual conduct or a romantic relationship with a student. [See Board Policy DF]

Upon request from administration, an employee will provide the phone number(s), social network site(s), or other information regarding the method(s) of electronic media the employee uses to communicate with any one or more currently-enrolled students.

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 social media sites. 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.

Student Participation in Social Media

A student may use District technology resources to participate in social media with parental consent and only as approved by the District in accordance with the student's age, grade level, and approved instructional objectives. This includes text messaging, instant messaging, email, web logs (blogs), electronic forums (chat rooms), video-sharing websites (e.g., YouTube), editorial comments posted on the internet, and approved social networking sites.

Student Training on Safety and Security

Students participating in social media using the District's technology resources will receive training to:

- Assume that all content shared, including pictures, is public;

- Not share personally identifiable information about themselves or others;
- Not respond to requests for personally identifiable information or respond to any contact from unknown individuals;
- Not sign up for unauthorized programs or applications using the District's technology resources;
- Understand the risks of disclosing personal information on websites and applications using the students' own personal technology resources; and
- Use appropriate online etiquette and behavior when interacting using social media or other forms of online communication or collaboration.

[See Reporting Violations, below]

Approval of Technology Resources

The District will ensure that all technology resources in use in the District meet state, federal, and industry standards for safety and security of District data, including a student's education records and personally identifiable information. [See FL]

Before use in the classroom, use with students, or administrative use, any professional staff wanting to use an online learning resource, online or mobile application, digital subscription service, or other program or technology application requiring the user to accept terms of service or a user agreement, other than a District-approved resource, must first submit an application for approval.

If approved, additional parental notification or permission may be required before use by students.

No student 13 years of age or younger will be asked to download or sign up for any application or online account using his or her own information. For elementary students, only applications that allow for one classroom or administrator-run account will be approved.

Reporting Violations

All users must immediately report any known or suspected violation of the District's applicable policies, cybersecurity plan, internet safety plan, or acceptable-use guidelines to a supervising teacher, the technology coordinator, or Superintendent, as appropriate.

Students and employees must report to a supervising teacher or the technology coordinator any requests for personally identifiable information or contact from unknown individuals, as well as any content or communication that is abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.

The technology coordinator will promptly inform the Superintendent, law enforcement, or other appropriate agency of any suspected illegal activity relating to misuse of the District's technology resources and will cooperate fully with local, state, or federal officials in any investigation or valid subpoena. [See GR series and CQB]

Loss of Privileges

Inappropriate use of the District's technology resources may result in revocation or suspension of the privilege to use these resources, as well as other disciplinary or legal action, in accordance with applicable laws, District policies, the Student Code of Conduct, and District administrative regulations. [See DH, FN series, and FO series]

The District has designated the following staff person as the technology coordinator:

Dustin Hardin
Chief Technology Officer
dhardin@ccisd.net
(281) 284-0401

The technology coordinator for the District's technology resources (or campus designee) will:

1. Assist in the development and review of responsible-use guidelines, the District's internet safety plan, the District's cybersecurity plan, and the District's security breach prevention and response plan. [See CQB]
2. Be responsible for disseminating, implementing, and enforcing applicable District policies and procedures, the internet safety plan, the acceptable-use guidelines for the District's technology resources, and the District's breach-prevention and response plan.
3. Provide training to all users regarding safe and appropriate use of the District's technology resources, including cyberbullying awareness and response, data security, and cybersecurity measures. The technology coordinator or designee will provide training to all employees within 30 days of hire and will provide annual training to all employees.
4. Collect and maintain evidence related to incidents involving the District's technology resources, as requested by the administration.
5. Notify the appropriate administrator of incidents requiring District response and disciplinary measures, including incidents of cyberbullying.

6. Ensure that all software loaded on computers in the District is consistent with District standards and is properly licensed. [See CY]

7. Be authorized to monitor or examine all system activities, including electronic mail transmissions, as deemed appropriate to ensure student safety online and proper use of the District's technology resources.

8. Coordinate with the District's records management officer to develop and implement procedures for retention and security of electronically stored records in compliance with the District's records management program. [See CPC]

9. Coordinate with the District webmaster to maintain District, campus, and classroom websites, consistent with the District's policies. [See BBE, CPC, CQA, and CY]

10. Coordinate with the District's cybersecurity coordinator about any known or suspected cybersecurity violations.

11. Set limits for data storage as needed.

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. 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. Emails will be purged from the system after two years and must be retained by the user if required to be retained longer than two years. 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.

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.

Use of Student Personal Electronic Devices for Instructional Purposes

The following rules will apply to student use of personal telecommunications or other electronic devices for on-campus instructional purposes:

1. Agreements for acceptable use of the District's technology resources and personal telecommunications or other electronic devices for on-campus instructional purposes must be signed annually by both the student and the parent.
2. Students must follow the rules and guidelines for technology use as published in the student handbook, policy FNCE, and in compliance with applicable administrative regulations, guidelines and user agreements.
3. District staff should avoid troubleshooting or attempting to repair a student's personal electronic device. The District is not responsible for damages.
4. The District is not responsible for damage to or loss of devices brought from home.

Violation of these rules may result in suspension or revocation of system access and/or suspension or revocation of permission to use personal electronic devices for instructional purposes while on campus, as well as other disciplinary action, in accordance with the Student Code of Conduct.

Email Ownership

All email accounts maintained on 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 should exist in anything created, stored, sent or received on the district's systems. 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 or schemes to compromise identity. 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.

Approved Mobile Devices

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 personally-owned mobile devices, however information can be found on the employee portal to set up a personally owned device.

Issuing Equipment to Students

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

1. Proposals to distribute devices and equipment to students must be submitted to the Chief Technology Officer for initial approval.
2. In loaning devices and equipment to students, the principal will give preference to educationally disadvantaged students as defined by the Education Code.
3. Before loaning devices and equipment to a student, the campus technology coordinator and principal must have clearly outlined a process that includes:
    a. Criteria to determine eligibility of students;
    b. An application that identifies the responsibility of the student regarding home placement, use, and ownership of the device or equipment;
    c. Procedures for distributing and initially training students in the setup and care of the device or equipment;

d. Provision of technical assistance for students using the device or equipment;

e. Criteria to determine continuation of student use of the device or equipment;

f. Documented assessment of any impact on student achievement that use of the device or equipment may provide; and

4. Procedures for retrieval of the device or 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.