The Superintendent or designee will oversee technology resources. For this regulation, “technology resources” means electronic communication systems and electronic equipment.

The District will make technology resources available to staff, students, parents, and the members of the public, as applicable. Available technology resources include onsite internal 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 District will develop and implement an Internet Safety Plan, including responsible use guidelines for the use of the District’s technology resources. All users will be provided copies of responsible use guidelines and training for proper use of the District’s technology resources. All training in the use of the District’s technology resources will emphasize ethical and safe use.

CONSENT REQUIREMENTS

No original work created by any District student will be posted on a web page under the District’s control unless the District has received written consent from the guardian of the student 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 guardian. An exception may be made for “directory information” as allowed by the Family Educational Rights and Privacy Act (FERPA) and District policy. [See CQ and policies at FL]

FILTERING

The Superintendent or designee will appoint a committee to select, 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/pornography; images or descriptions of sexual acts; promotion of violence, illegal use of weapons, drug use, discrimination, or participation in hate groups; instructions for performing criminal acts (e.g., bomb making); and online gambling.

REQUEST TO DISABLE FILTER

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

SYSTEM ACCESS

Access to the District’s technology resources will be governed as follows:

GENERAL GUIDELINES

1. All students, employees, and Board members will be required to sign an acceptable use agreement annually for issuance or renewal of an account.
2. Students granted access to the District's technology resources must complete any applicable user training, including training on cyberbullying awareness and response, and appropriate online behavior and interactions with other individuals on social networking websites.
3. A teacher may apply for a class account and in doing so will be ultimately responsible for use of that account.
4. The District will require that all employees' passwords be changed at least every 180 days.
5. Any user identified as a security risk or as having violated District and/or campus computer use guidelines may be denied access to the District's technology resources and will be subject to disciplinary action and criminal prosecution.
6. All nonschool users using the District's technology resources will comply with the District's acceptable use guidelines.
7. Resources are to be used mainly for educational and administrative purposes, but some limited personal use is permitted.
8. District-owned devices and personal devices that allow access to District e-mail or potentially sensitive student or employee records must be password protected.

STUDENT TRAINING ON SAFETY AND SECURITY

9. Students in K–grade 5 will be granted access to the District's technology resources as determined by the campus principal.

   Elementary students will have access to District-managed online educational applications and will not be issued or asked to create individual accounts using personally identifiable information.

   Elementary students in K–grade 5 may have access to District-issued network accounts or e-mail (restricted to internal communications) only as approved by the campus principal.

   Students in grades 6–12 will be assigned individual accounts and passwords for use of District-sponsored technology resources, including individual e-mail accounts and District-approved online educational resources.

DISTRICT EMPLOYEES AND BOARD MEMBERS

10. 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.

11. Before use in the classroom, use with students, or administrative use, all digital subscriptions, online learning resources, online applications, or any other program requiring the user to accept terms of service or a user agreement must be approved by Technology Services.

    District staff and Board members should not accept terms and conditions or sign user agreements on behalf of the District without preapproval.

12. Teachers and other professional staff may request to use additional online technology resources for instructional and administrative use as described below in the section labeled APPROVAL OF TECHNOLOGY RESOURCES.

MEMBERS OF THE PUBLIC

13. Members of the public may be given access to District technology resources, 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 administrative department.

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

A student may use District technology resources to participate in social media 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, e-mail, weblogs (blogs), electronic forums (chat rooms), video-sharing websites (e.g., YouTube), editorial comments posted on the Internet, and approved social network sites.

STUDENT PARTICIPATION IN SOCIAL MEDIA

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

1. Assume all content shared, including pictures, is public;

2. Not share personally identifiable information about themselves or others;

3. Not respond to requests for personally identifiable information or respond to any contact from unknown individuals;

4. Not sign up for unauthorized programs or applications using the District's technology resources;

5. Understand the risks of disclosing personal information on websites and applications using the students' own personal technology resources; and

6. Use appropriate online etiquette and behavior when interacting using social media or other forms of online communication or collaboration.

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

Before use in the classroom, use with students, or administrative use, professional staff wanting to use an online learning resource, online 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.

APPROVAL OF TECHNOLOGY RESOURCES

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

Students must immediately report to a supervising teacher, and employees must immediately report to their principal or department head, the following:

1. Any known violation of the District's applicable policies, Internet safety plan, or responsible use guidelines.

2. Requests for personally identifying 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 Chief Information Officer will promptly inform the Superintendent, law enforcement, or other appropriate state agency of any suspected illegal activity relating to the 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(LEGAL)]

SANCTIONS

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 ap-

plicable laws, District policies, the Student Code of Conduct, and District administrative regulations. [See DH, FN, and FO series]

REVOCATION OF USE

Termination of a student's access will be effective on the date the principal receives notice of a student's withdrawal or revocation of system privileges.

Termination of a staff member's access will be effective on the date the principal or District supervisor receives notice of a staff member's resignation, termination, retirement, or revocation of system privileges. The effective date may be a future date if so specified in the notice.

NETWORK SECURITY

All additions and changes to the District's network must be coordinated with technology services in order to ensure overall compatibility and to meet District security requirements as follows:

1. Points of Entry: No external network connections will be made to or from the District's network without authorization from Technology Services. This includes connections such as dial-ups, leased lines, wireless access points, proxy servers, relay servers, file-sharing networks, and the like.
2. Network Servers: Installation and usage of all networked servers and associated network services (i.e., file, print, DHCP, DNS, FTP, and the like) must be approved by technology services to ensure compliance for data security, network integration, and software licensing.
3. Administrative Software: The use of server and network administrative software on the District's network is prohibited. This includes software such as network packet analyzers, network security discovery tools, and server administrative applications.
4. Network Devices: The addition and/or relocation of all devices that connect to the District's network must be coordinated with technology services. This includes all desktop computers, printers, telephones, projectors, networking equipment, and the like.
5. Access Control: Any employee attempting to gain access to computers, servers, and/or network switches, routers, and the like, even if said systems lack physical or electronic barriers for access (e.g., a closet door left open inadvertently or a system missing a password), other than to perform his or her job functions will be subject to disciplinary action including suspension without pay or termination of employee or contract.

CHIEF INFORMATION OFFICER RESPONSIBILITIES

The District's chief information officer (or campus/departmental designee) will:

1. Assist in the development and review of responsible use guidelines, the District's Internet safety plan, and the District's Data Breach Prevention and Response Plan.
2. Be responsible for disseminating and enforcing applicable District policies, the Internet safety plan, and responsible use guidelines for the District's technology resources and the District's Data Breach Prevention and Response Plan.
3. Ensure that all software loaded on computers in the District is consistent with District standards and is properly licensed.
4. 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.
5. Be authorized to disable a content filtering device on the system for bona fide research or another lawful purpose, with approval from the Superintendent or designee.
6. Be authorized to establish a retention schedule for messages on any electronic bulletin board and to remove messages posted locally that are deemed inappropriate.
7. Set limits for data storage within the District's system, as needed.
8. Collect and maintain evidence related to incidents involving District technology resources, as requested by the administration.
9. Notify the appropriate administrator of incidents requiring District response and disciplinary measures, including incidents of cyberbullying.
10. Provide ongoing training to all users regarding safe and appropriate use of the District's electronic resources, including cyberbullying awareness and response.
11. Ensure that employees supervising students who use the District's technology resources provide training emphasizing the safe and appropriate use of this resource.
12. Ensure that all users of the District's technology resources annually complete and 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.

13. Coordinate with the District's record management officer to develop and implement procedures for record retention of electronically stored records and establish a retention schedule for messages that are considered local government records.

The following standards will apply to all users of the District's technology resources. Users who violate these standards may be subject to disciplinary action in accordance with District policies and/or administrative regulations:

1. The individual in whose name a system account is issued will be responsible at all times for its proper use and for not sharing his or her login name or password for that account with others.

2. Users granted access to generic mail accounts will be responsible at all times for its proper use. Any generic accounts are the responsibility of the appropriate principal/department head and his or her designee.

3. The District's technology resources may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy.

4. Users may not use another person's ID or password.

5. Users may not upload or download programs to or from the District's technology resources without appropriate authorization.

6. Users may not use the network in such a way that would disrupt the use of the network by other users.

7. Users must not violate other users' intellectual property rights by redistributing 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.

8. If a user identifies or has knowledge of a security problem on the network, the user must notify a system administrator. The security problem should not be shown or demonstrated to other users.

9. Unbridled and open-ended use of the network cannot be accommodated as financial resources remain finite. Users are required to exercise prudence in the use of this shared resource.

10. E-mail communication is not secure. Any user sending personally identifying data, such as social security numbers and birth dates, for valid business reasons must encrypt the data before transmitting.

11. Users may not disable, attempt to disable, or bypass any controls and/or filters that the District has established.

12. Users may not gain unauthorized access to resources or information.

13. Students may not respond to requests for personally identifying information or contact from unknown individuals.

14. Users may not pretend to be someone else when sending/receiving messages.

15. Users may not use inappropriate language such as swear words, vulgarity, ethnic or racial slurs, or any other inflammatory language.

16. Users may not send, post, or possess materials that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal; including material that constitutes cyberbullying and "sexting." Users who access such material are expected to discontinue the access as quickly as possible and to report the incident to a supervising teacher and/or technology coordinator.

17. Users may not use their District-issued e-mail accounts to subscribe to mailing lists or services that are not educational publications or for instructional or job-related functions.

18. Only those employees or officials expressly authorized to speak to the media or public on behalf of the District may represent the District in such communications via e-mail messages.

19. Users may not access the resources to knowingly alter, damage, or delete District property or information, or to breach any other electronic equipment, network, or electronic communications system in violation of the law or District policy.

20. Users may not damage or vandalize electronic communication systems or electronic equipment, including knowingly or intentionally introducing a virus to a device or network, or not

taking proper security steps to prevent making a device or network vulnerable, such as opening e-mail messages from unknown senders and loading data from unprotected sources.

21. Communications may not be encrypted so as to avoid security review by system administrators.

22. Users may not use another person's account without written permission from the campus administrator or District administrator, as appropriate.

23. Users may not attempt to read, delete, copy, modify, or interfere with another user's posting, transmittal, or receipt of electronic media.

24. Students may not use e-mail or websites to engage in or encourage illegal behavior or to threaten school safety.

25. Students should never make appointments to meet people whom they meet online and should report to a teacher or administrator if they receive any request for such a meeting.

26. Users may not post or transmit pictures of students without obtaining prior authorization from all individuals depicted or from parents of depicted students who are under the age of 18.

27. Users should be mindful that use of school-related e-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.

28. Users may not waste the District's technology resources, including sending spam.

29. Users must purge electronic records in accordance with established retention guidelines. [See BBE and CPC]

EDUCATION, SUPERVISION, AND MONITORING

It will be the responsibility of all members of the District to educate, supervise, and monitor appropriate usage of the online computer network and access to the Internet in accordance with the Children's Internet Protection Act (CIPA).

MONITORED USE

All Internet activities, electronic mail transmissions, and other use of the District's technology resources are not confidential. To ensure appropriate use, all such activities and communications are automatically logged and monitored for compliance. Designated District staff will be authorized to monitor the District's technology resources at any time to ensure appropriate use.

All communication over District resources is subject to disclosure under the Texas Public Information Act.

E-mails regarding District business sent to or from an employee's personal (private, not District) e-mail account, personal computer, private social networking page, and the like may be public record.

VANDALISM PROHIBITED

Any attempt to harm or destroy District equipment or materials, data of another user of the District's electronic system(s), or 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 possibly 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, hardware, or software costs. [See DH, FN series, FO series, and the Student Code of Conduct]

ETIQUETTE

In addition to standards for online conduct, users of the District's technology resources are expected to observe the following standards for etiquette:

1. Be polite; messages typed in capital letters are the computer equivalent of shouting and are considered rude.
2. Be considerate when sending e-mail attachments by taking into account whether a file may be too large to be accommodated by the recipient's technology resources or may be in a format unreadable by the recipient.
3. Do not use the District's technology resources in such a way that would disrupt use for others.

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 or deliberate interference with the ability of other system users to send/receive electronic mail 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 District'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 District's electronic environment will be subject to disciplinary action in accordance with District policies. [See DH]

PARTICIPATION IN SOCIAL NETWORKING WEBSITES AND CHAT ROOMS

Participation in social media using the District's technology resources for educational and administrative purposes is permissible for students, under appropriate supervision.

Social networking/media includes text messaging, instant messaging, electronic mail (e-mail), web logs (blogs), electronic forums (chat rooms), video-sharing websites (e.g., YouTube), editorial comments posed on the Internet, and social network sites (e.g., Facebook, MySpace, Twitter, LinkedIn).

Employees are strictly forbidden from communicating with students from their personal social networking sites (i.e., inviting students or accepting invitations from students). An employee is not subject to these provisions to the extent an 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.

Accessing personal social networking websites and/or chat rooms from the District's network is strictly prohibited, except during reasonable periods of time such as coffee and lunch breaks. All social networking activities are monitored and logged for compliance, even if they are personal.

Participation in social networking websites and/or chat rooms is permissible for students and employees under the following conditions:

1. A completely separate "professional" site may be created by employees specifically for the purposes of interacting with students strictly for instructional and curricular (or extracurricular) activities. Such "professional" sites should be limited to certified or licensed employees who work directly with students due to their instructional or curricular (extracurricular)

roles or to any other employee so designated by the Superintendent or principal. All other employees are prohibited from communication through social networking sites with students who are enrolled in the District.

2. Employees will not communicate directly with any student between the hours of 10:00 p.m. and 6:30 a.m. Exceptions include extracurricular/curricular activities, field trips, and emergency situations that may require contact before 6:30 a.m. or after 10:00 p.m.

3. Employees will refrain from inappropriate communication with students. Factors considered in assessing whether the communication is inappropriate include but are not limited to:

    a. Nature, purpose, timing, and amount of communication;

    b. The subject matter of the communication;

    c. Whether the communication was made openly or attempted to conceal;

    d. Whether the communication was sexually explicit; and

    e. Whether the communication could be interpreted as soliciting sexual contact or a romantic relationship.

4. Administrators may require staff to include an administrator or designee to be copied on texts sent to students.

5. Employees will limit such communications to school-related business or to matters that fall within the scope of the employees' professional responsibilities. Such sites must be open to the administration, parents, and guardians.

6. Employees granting access to students on instructional social networking sites will limit communications to school-related business or to matters that fall within the scope of the employees' professional responsibilities. Such sites must be open to the administration, parents, and guardians.

7. Employees granting access to students on instructional social networking sites will comply with record retention and destruction requirements that apply to electronic media.

8. Without parental permission, pictures or information regarding students should not be on instructional social networking sites (subject to FERPA).

9. Employees must comply with the Public Information Act and the FERPA, including retention and confidentiality of student and District records.

10. Employees must adhere to professional and District standards of conduct when posting information to the Internet and in communication with students.

11. Employees granting access to students on public social networking sites should be aware that all correspondence related to District business on these sites may be subject to disclosure under the Texas Public Information Act.

12. Students and employees participating in social networking websites or chat rooms using District electronic resources should assume that all content shared, including pictures, is public.

13. No personally identifying information should be published.

14. Students should not respond to requests or send personally identifying information or any communications to unknown individuals.

15. Information about the date, time, and location of District field trips should not be shared.

DISTRICT WEBSITE

The District will maintain a District website 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 website must be directed to the designated webmaster. The community relations officer and the District webmaster will 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.

No commercial advertising will be permitted on a website controlled by the District.

CAMPUS SOCIAL MEDIA SITES

Schools that have digital or social media sites (YouTube, Facebook, Twitter, and the like) must provide a link to these sites from their campus home page. Campus principals and assigned campus staff are responsible for the monitoring of these sites.

Any site found to have offensive content or that is not in alignment with District policy will be reported immediately to the District webmaster.

If a campus finds an unauthorized digital or social media site that is identifying itself as an official campus communication, the campus will immediately forward this information to the District webmaster.

SCHOOL OR CLASS WEB PAGES

Schools or classes may publish and link to the District's website pages that present information about the school or class activities, subject to approval from the webmaster. The campus principal will designate the staff member responsible for managing campus web pages under the supervision of the District webmaster. Teachers will be responsible for compliance with District rules in maintaining their class web pages. Any links from a school or class web page to sites outside the District's computer system must receive approval from the District webmaster or designated staff member assigned to manage the campus page.

Information about the date, time, and location of District field trips should not be shared.

STUDENT WEB PAGES

Students will not be permitted to publish personal web pages using District resources unless such web pages are required as part of the curriculum. If required as part of the curriculum, all material presented on a student's web page must be related to the student's educational activities. Student web pages must include the following notice: "This is a student web page. Opinions expressed on this page shall not be attributed to the District." Any links from a student's web page to sites outside the District's computer system must receive approval from the District webmaster or designated staff member assigned to manage the campus page.

TEACHER WEB PAGES

All teachers are required to have a teacher page or curriculum/grade-level page. All pages will have the following information and should be updated on a regular basis:

- Teacher name;
- Contact information;
- Short biography; and
- General class information, which may include class schedule, tutorial times and dates, assignments, and homework.

Teachers who are using blogs, social media, or any other external web page as part of their class instruction must provide links to these web pages under the Resources listing. It is the responsibility of the teacher or grade-level team to monitor the content of these links to ensure they are in compliance with District technology policies. Any external links that are not in alignment with District policy will be removed.

ADMINISTRATOR WEB PAGES

All campus administrators are required to have a web page that provides information for parents and the community.

All pages will have the following information and should be updated on a regular basis:

- Administrator's name;
- Contact information;
- Short biography; and
- General campus information, which may include semester message, campus newsletter, and events calendar.

Administrators who are using blogs, social media or any external web page as part of the campus communications must provide links to these web pages under the Resources listing. (Example: Twitter, Facebook, blog, and the like) It is the responsibility of the administrator to monitor the content of these links to ensure they are in compliance with District technology policies. Any external links that are not in alignment with District policy will be removed.

EXTRACURRICULAR ORGANIZATION WEB PAGES

With the approval of the District webmaster or campus principal, extracurricular organizations may establish web pages linked to or from a campus or District website; however, all material presented on the web page must relate specifically to the organization activities and include only student-produced material. The sponsor of the organization will be responsible for compliance with District rules for maintaining the page.

Web pages of extracurricular organizations must include the following notice: "This is a student extracurricular organization web page. Opinions expressed on this page shall not be attributed to the District."

Any links from the web or page of an extracurricular organization to sites outside the District's computer system must receive approval from the District webmaster, department site owner, or campus principal.

PERSONAL WEBSITE

A staff member who maintains a personal website not provided by the District may not:

1. Link to or replicate content of the official Spring Branch ISD website without written permission of the District;
2. State or imply in any manner that it is an "official" website of the District;
3. Imply that it is endorsed by the District; and
4. Present false information about the District or its programs, policies, or practices.

COPYRIGHT COMPLIANCE

The use of District technology in violation of any law, including copyright law, is prohibited. Copyrighted or licensed software or data may not be placed on any system connected to the District's system without written permission from the holder of the copyright or license. Only the copyright of the license owner, or an individual the owner specifically authorizes, may upload copyrighted or licensed material to the system.

No person will be allowed to use the District's technology to post, publicize, or duplicate information in violation of copyright law.

RECORD RETENTION

A District employee will retain electronic records, whether created or maintained using the District's technology resources or using personal technology resources, in accordance with the District's record management program. [See CPC]

DISCLAIMER OF LIABILITY

The District's technology resources are 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 District's technology resources and any information or software contained therein. The District does not warrant the functions or services performed by, or that the information or software contained as part of, the District's technology resources will meet the system user's requirements or that the system will be uninterrupted, 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 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 technology resources and will cooperate fully with law enforcement in response to any investigation or valid subpoena.

The District will not be liable for users' inappropriate use of the District's technology resources, violations of copyright restrictions or other laws, users' mistakes or negligence, or costs incurred by users. The District will not be responsible for ensuring the availability of the District's resources or the accuracy, age appropriateness, or usability of any information found on the Internet.

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. Proposed projects to distribute devices and equipment to students must be submitted to the campus principal or designee for initial approval.
2. A student is eligible to receive devices and equipment under these rules only if the student does not otherwise have home access to these resources, as determined by the principal and school counselor, or if the student is issued equipment through a special program.
3. In loaning devices and equipment to students, the principal will give preference to educationally disadvantaged students.
4. Students taking devices home for use on their home network will not have access to District filters. Parents are responsible for monitoring students' Internet activity and ensuring proper use of the Internet.
5. Before loaning devices and equipment to a student, the campus principal must have clearly outlined:
    a. A process to determine eligibility of students;
    b. An application process that identifies the responsibility of the student regarding home placement, use, and care of the device or equipment;
    c. A process to distribute and initially train students in the setup and care of the device or equipment;
    d. A process to provide ongoing technical assistance for students using the device or equipment; and
    e. A process for retrieval of the device or equipment from a student, as necessary.

USE OF PERSONAL TELECOMMUNICATIONS OR OTHER 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 responsible 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. [See CQ(EXHIBIT)]
2. When not using devices for instructional purposes while on campus, students must follow the rules and guidelines for non-instructional use as published in the student handbook and policy FNCE.

3. District staff should avoid troubleshooting or attempting to repair a student's personal electronic device. The District is not responsible for damages.

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.