ELECTRONIC COMMUNICATION AND DATA MANAGEMENT
CQ (REGULATION)

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

The District will provide training in proper use of the systems and will provide all users with copies of acceptable use guidelines. All training in the use of the District's systems will emphasize the ethical and safe use of these resources.

CONSENT REQUIREMENTS

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 "directory information" as allowed by the Family Educational Rights and Privacy Act and District policy. [See FL (Legal & Local).]

FILTERING

The Superintendent will appoint a committee, to be chaired by the technology director, to select, implement, and maintain appropriate technology for filtering Internet sites containing material considered inappropriate or harmful to minors. All Internet access will be filtered for minors and adults on 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 on-line gambling.

PERSONAL TECHNOLOGY RESOURCES

Students, employees, and guests may connect personal technology resources to the District network for educational purposes as set forth by the Superintendent or designee. [See FNCE for student use of personal electronic devices for instructional purposes]

SOFTWARE

All software used in the District must be legally licensed and approved. All district software shall be installed by technology staff or a designee.

DONATED HARDWARE RESOURCES

Donated technology resources may be accepted if the equipment meets or exceeds the minimum standards as set forth by the Superintendent or designee. All donated technology resources shall become the property of the District.

DONATED SOFTWARE RESOURCES

Software may be accepted as a donation to the District if the software meets the standards as set forth by the Superintendent or designee. All donated software shall become the property of the District and shall be installed by technology department staff or a designee.

REQUESTS TO UNBLOCK SITES

The Superintendent's designee will consider requests from users who wish to use a blocked site for bona fide research or other lawful purposes.

SYSTEM ACCESS

Access to the District's technology resources, including the Internet, shall be made available to students, employees, and members of the community primarily for instructional and administrative purposes and in accordance with administrative regulations.

All users shall be prohibited from using the network resources for personal gain or commercial work.

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

All users will be required to sign an acceptable use agreement annually, or as determined by the Superintendent's designee, for issuance or renewal of an account.

Students will be granted access to the District's system by a teacher or administrator, as appropriate, after signing the acceptable use agreement. Students will not be assigned an individual account or password for e-mail purposes. Students granted access to the District's system must complete any applicable District network training.

District employees will be granted access to the District's system as appropriate and with the approval of the immediate supervisor and after completion of District network training and signing the acceptable use agreement and/or other required agreements. Employees may not be provided access to the District's system from their personal computers without the written approval of the technology director and the employee's supervisor. The District assumes no responsibility for membership, charges or costs associated with home use by employees. Employees may not use the District's system for personal or commercial use, with the exception of limited personal use of the District's e-mail system.

Members of the Board of Trustees will be granted access to the electronic communications system during their terms of office. Members will also be loaned District computer equipment to enable them to communicate through the electronic communications system during their terms of office.

The District will require that all passwords be changed frequently. All passwords must remain confidential and should not be shared.

Any system 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 system.

ACCEPTING ELECTRONIC SIGNATURES

The District may accept electronically signed documents or digital signatures for any transactions and purposes allowed by law, including contracts for goods and services, student admissions documents, and employment documents.

The District will comply with rules adopted by the Department of Information Resources (DIR), to the extent practicable, to:

- Authenticate a digital signature for a written electronic communication sent to the District;
- Ensure that records are created and maintained in a secure environment;
- Conduct risk assessments for transactions involving digital signatures;
- Implement appropriate nonrepudiation services; and
- Maintain all records as required by law.

TECHNOLOGY DIRECTOR RESPONSIBILITIES

The technology director and/or campus administrators will:

1. Be responsible for disseminating and enforcing applicable District policies and acceptable use guidelines for the District's system.
2. Ensure that all users of the District's system 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.
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 transmissions, as deemed appropriate to ensure student safety online and proper use of the system.

6. Be authorized to unblock Internet sites for bona fide research or another lawful purpose.
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.

INDIVIDUAL USER RESPONSIBILITIES

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

ONLINE CONDUCT

1. The individual in whose name a system account is issued will be responsible at all times for its proper use.
2. Students completing required course work on the system will have priority use.
3. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy or guidelines.
4. System users may not disable, or attempt to disable, a filtering device on the District's electronic communications system.
5. Communications may not be encrypted so as to avoid security review by system administrators.
6. System users may not use another person's system account without written permission from the campus administrator or District coordinator, as appropriate.
7. Students may not distribute personal information about themselves or others by means of the electronic communications system; this includes, but is not limited to, personal addresses and telephone numbers.
8. 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.
9. System users must purge electronic mail in accordance with established retention guidelines.
10. System users may 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 should avoid actions that are likely to increase the risk of introducing viruses to the system, such as opening e-mail messages from unknown senders and loading data from unprotected computers.
12. System users may not upload or download programs to the system unless authorized by the technology director or designee. Users may not load programs not owned by the District on a District computer.
13. System users may not send or post messages that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
14. System users may not purposefully access materials that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.

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 may not waste District resources related to the electronic communications system.
17. System users may not gain unauthorized access to resources or information.
18. System users identifying a security problem in the system must notify the appropriate teacher, campus administrator, or technology directory.

VANDALISM PROHIBITED

Any malicious attempt to harm or destroy District equipment or data or the 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. [See DH, FN series, FO series, and the Student Code of Conduct.]

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 user 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.

Any user who gains access to such material is expected to discontinue the access as quickly as possible and to report the incident to a teacher, in the

case of a student, or a supervisor or the technology director, in the case of an employee.

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 educational chat rooms and newsgroups accessed on the Internet is permissible for students, under appropriate supervision, if approved by the technology director.

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 designated Webmaster. The technology director 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 Web site controlled by the District without written permission from the student's parent.

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

CAMPUS OR CLASS WEB PAGES

Campuses or classes may publish and link pages to the District's Web site to 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 the campus's Web page under the supervision of the campus principal and the District's 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.

EXTRA-CURRICULAR ORGANIZATION WEB PAGES

With the approval of the District Webmaster, extra-curricular organizations may establish Web pages linked to a campus or District Web site; however, all material presented on the Web page must relate specifically to student and/or organization activities. The sponsor of the organization will be responsible for compliance with District rules for maintaining the Web 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 page of an extracurricular organization to sites outside the District's computer system must receive approval from the District Webmaster.

PERSONAL WEB PAGES

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

NETWORK ETIQUETTE

System users are expected to observe the following network etiquette:

1. Be polite; messages typed in capital letters are the computer equivalent of shouting and are considered rude.

2. Use appropriate language; swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language are prohibited.

3. Pretending to be someone else when sending/receiving messages is considered inappropriate.

4. Transmitting obscene messages or pictures is prohibited.

5. Be considerate when sending attachments with e-mail by considering whether a file may be too large to be accommodated by the recipient's system or may be in a format unreadable by the recipient.

6. Using the network in such a way that would disrupt the use of the network by other users is prohibited.

TERMINATION / REVOCATION OF SYSTEM USER ACCOUNT

Termination of an employee's or a student's access for violation of District policies or regulations will be effective on the date the principal or District administrator receives notice of 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 express 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.

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 permission from the holder of the copyright or license. Only the copyright or 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. The technology director will use all reasonable measures to prevent the use of District technology in violation of the law

COMPLAINTS REGARDING COPYRIGHT COMPLIANCE

If a copyright or license owner reasonably believes that the District's technology has been used to infringe upon a copyright or license, the owner is encouraged to notify the Superintendent's office.

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 projects to distribute computer equipment to students must be submitted to the appropriate executive director or assistant superintendent for approval.

2. A student is eligible to receive computer equipment under these rules only if the student does not otherwise have home access to computer equipment, as determined by the principal and counselor.

3. In transferring computer equipment to students, the principal will give preference to educationally disadvantaged students.

4. Before transferring computer 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 ownership of the equipment;
    c. A process to establish that all software on the computer at the time of transfer is legally licensed.
    d. A process to distribute and initially train students in the setup and care of the equipment;
    e. A process to provide ongoing technical assistance for students using the equipment;
    f. A process to determine ongoing student use of the equipment;
    g. A process to determine any impact on student achievement the use of this equipment may provide; and
    h. A process for retrieval of the equipment from a student, as necessary.

APPROVED – NOVEMBER 2015