UNITED INDEPENDENT SCHOOL DISTRICT

AGENDA ACTION ITEM

TOPIC Second Reading of Policy CQ (LOCAL) – Technology Resources

SUBMITTED BY: Hector Perez OF: Ex. Director for Technology

APPROVED FOR TRANSMITTAL TO SCHOOL BOARD: ______________________

DATE ASSIGNED FOR BOARD CONSIDERATION: June 20, 2012

RECOMMENDATION:

It is recommended that the Board of Trustees approve Second Reading of Policy CQ (LOCAL): Technology Resources

RATIONALE:

BUDGETARY INFORMATION:

BOARD POLICY REFERENCE AND COMPLIANCE:

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 employee handbook. For information regarding District, campus, and classroom Web sites, see CQA. For information regarding intellectual property and copyright compliance, see CY.

The Superintendent or designee and the technology coordinator will oversee the District's technology resources, meaning electronic communication systems and electronic equipment.

The District will develop and implement acceptable use guidelines and an Internet safety plan. All users will be provided copies of acceptable use guidelines and training in 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.

FILTERING

The Superintendent will appoint a committee, to be chaired by the technology coordinator, 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.

ACCESS

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

1. Students in grades **Pre-Kinder through 12th grades** will be assigned individual accounts.
2. Students granted access to the District's technology resources must complete any applicable user training.

3. As appropriate and with the written approval of the immediate supervisor and completion of District network training, District employees will be granted access to the District's technology resources.

4. A teacher may apply for a class account and in doing so will be ultimately responsible for use of the account.

5. The District will require that all passwords be changed every ~~-~~**180 days**. All passwords must remain confidential and should not be shared.

6. 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.

7. All ~~students,~~ employees~~,~~ and Board members will be required to sign an acceptable use agreement~~-f~~ annually for issuance or renewal of an account.

~~7.~~8. **Students will be required to sign an acceptable use agreement at the time of initial enrollment, ~~- and at middle school and high school transitional periods, i.e.~~upon transition from elementary to middle school, and upon transition from middle school to high school.**

~~8.~~9. All nonschool users will be required to sign an acceptable use agreement before being granted access.

~~9.~~10. Resources are to be used mainly for educational and administrative purposes, but some limited personal use is permitted.

STUDENT PARTICIPATION IN SOCIAL MEDIA

Participation in any social media using the District's technology resources is not permissible for students.

TECHNOLOGY COORDINATOR RESPONSIBILITIES

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

Name: **Hector Perez**

Position: **Executive Director of Information Technology**

Telephone: **956-473-6370**

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

1. Assist in the development of acceptable use guidelines and the District's Internet safety plan.

2. Be responsible for disseminating and enforcing applicable District policies, the Internet safety plan, and acceptable use guidelines for the District's technology resources.

3. 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 agreements will be maintained on file in the principal's or supervisor's office.

4. Ensure that all users of the District's wireless Internet service acknowledge use terms.

5. Provide ongoing training to all users regarding safe and appropriate use of the District's technology resources, including cyberbullying awareness and response.

6. Ensure that employees supervising students who use the District's technology resources provide training emphasizing safe and appropriate use.

7. Collect and maintain evidence related to incidents involving the District's technology resources, as requested by the administration.

8. Notify the appropriate administrator of incidents requiring District response and disciplinary measures, including incidents of cyberbullying.

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

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

11. 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.

12. Coordinate with the District's record management officer to develop and implement procedures for record retention of electronically stored records.

13. Coordinate with the District Webmaster to maintain District Web sites.

14. Be authorized to establish a retention schedule for messages that are considered local governmental records and to remove messages from District, campus, and classroom Web sites that are deemed to be inappropriate, consistent with the District's record management program. [See BBE, CPC, and CQA]

15. Set limits for data storage, as needed.

INDIVIDUAL USER RESPONSIBILITIES

The following standards will apply to all users of the District's technology resources:

ONLINE CONDUCT

1. The individual in whose name an account is issued will be responsible at all times for its proper use and for not sharing the password for that account with others.

2. 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 or guidelines.

3. 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.

4. 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.

5. Users may not disable, or attempt to disable, any filtering device used by the District.

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

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

8. Users may not pretend to be someone else when posting, transmitting, or receiving messages.

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

10. Users may not engage in conduct that harasses or bullies others. [See DIA, FFH, and FFI]

11. 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 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.

12. ~~Students~~ **Users** may not use e-mail or Web sites to engage in or encourage illegal behavior or to threaten school safety.

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

14. ~~Students~~ **Users** may not distribute personal information about themselves or others by means of the District's technology resources; this includes, but is not limited to, personal addresses and telephone numbers.

15. ~~Students~~ **Users** may not respond to requests for personally identifying information or contact from unknown individuals.

16. 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.

17. Users may not post or transmit pictures of students without obtaining prior permission from all individuals depicted or from parents of depicted students who are under the age of 18. [See CQA(EXHIBIT) for release forms for the electronic display of original work and personal information]

18. 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. [See CY]

19. 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.

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

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

VANDALISM

Any malicious attempt to harm or destroy District equipment or data or the data of another user of the District's technology resources 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 or network viruses.

ETIQUETTE

In addition to the 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.

REPORTING VIOLATIONS

Students and employees must immediately report any known violation of the District's applicable policies, Internet safety plan, or acceptable use guidelines to ~~a supervising teacher~~ **an administrator** or the technology ~~coordinator~~ **department.**

Students and employees must report 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.

SANCTIONS

Inappropriate use of the District's technology resources may result in suspension or revocation 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]

TERMINATION / REVOCATION OF USE

Termination of access for violation of District policies or regulations will be effective on the date the principal or ~~District coordinator~~ **Technology Department** receives notice of withdrawal or of revocation of system privileges or on a future date if so specified in the notice.

DISCLAIMER

The District's technology resources are 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 District's technology resources 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 as part of, the District's technology resources will meet the user's requirements, or that the District's technology resources will be uninterrupted or error free, or that defects will be corrected.

Opinions, advice, services, and all other information expressed by 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. [See GR series]

ISSUING EQUIPMENT TO STUDENTS **FOR CLASSROOM USE**

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** p~~P~~**rincipal** for initial approval.

2. Before loaning devices and equipment to a student, the **D**~~d~~**istrict's** ~~campus~~ technology coordinator, **the Department of Curriculum and Instruction,** and principal must have clearly outlined:

~~a.~~ A process to determine **selection of class** ~~eligibility of students;~~

b. A process to distribute and initially train students in the setup and care of the device or equipment;

c. A process to provide ongoing technical assistance for students using the device or equipment;

d. A process to determine ongoing student use of the device or equipment;

e. A process to determine any impact on student achievement the use of the device or equipment may provide; and

f. 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. Requests to use personal telecommunications or other electronic devices for on-campus instructional purposes must be submitted to the c~~C~~ampus p~~P~~rincipal for initial approval. [See FNCE]

2. 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 by both the student and the parent. [See CQ(EXHIBIT)]

3. When using devices for instructional purposes while on campus, students must use the District's wireless Internet services and are prohibited from using a personal wireless service.

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.