Staff Use of Information Tech and Communications Resources Rules

~~District e~~Employees are expected to abide by the following rules when using information technology and communication resources:

A. Electronic Communications:
   1. Electronic communications are protected by the same laws and policies and are subject to the same limitations as other types of media. When creating, using, or storing messages on the network, the user should consider both the personal ramifications and the impact on the District should the messages be disclosed or released to other parties. Extreme caution should be used when committing confidential information to the electronic messages, as confidentiality cannot be guaranteed.

   2. The District may review email logs and/or messages at its discretion. Because all computer hardware, digital communication devices, and software belong to the District, users have no reasonable expectation of privacy, including the use of email, text-message and other forms of digital communications~~,~~ (e.g. voicemail, Twitter™, Facebook™, etc.) except as noted herein. The District may, through such review of email logs and/or messages, inadvertently obtain access information for an employee's personal internet account through the use of an electronic device or program that monitors the District's network or through an electronic communications device supplied or paid for in whole or in part by the District~~employer~~. If such personal internet access information is obtained by the District, the District will ~~shall~~ not use that access information to access the employee's personal internet account unless permitted by law.

   3. The use of the District's technology and electronic resources is a privilege which may be revoked at any time.

   4. Electronic mail transmissions and other use of the District's electronic communications systems or devices by employees shall not be considered confidential and may be monitored at any time by designated District staff to ensure appropriate use. This monitoring may include, but is not limited by enumeration to, activity logging, virus scanning, and content scanning. Participation in computer-mediated conversation/discussion forums for instructional purposes must be approved by the District Administrator, or designee~~curriculum or District administration~~. External electronic storage devices are subject to monitoring if used with District resources.

B. User Responsibilities: Network/Internet users ~~(students and District employees), like traditional library users or those participating in field trips,~~ are responsible for their actions in accessing available resources. The following standards will apply to all users ~~(students and employees)~~ of the network/Internet:
   1. The user, in whose name a system account is issued, will be responsible at all times for its proper use. Users may not access another person's account without written permission from the District Administrator, or designee~~an administrator or immediate supervisor~~.

2. The system may not be used for illegal purposes ~~, in support of illegal activities,~~ or for any other activity prohibited by District policy. ~~Doesn't "illegal purposes" include "support of illegal activities" if so, delete latter????~~

3. Users may not redistribute copyrighted programs or data without 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.

4. A user must not knowingly attempt to access educationally inappropriate material. If a user accidentally reaches such material, the user must immediately back out of the area on the Internet containing educationally inappropriate material. The user must then notify the building principal and/or immediate supervisor of the site address that should be added to the filtering software, so that it can be removed from accessibility.

5. A user may not disable Internet tracking software or implement a private browsing feature on District computers or networks. Browsing history must ~~shall~~ only be deleted by authorized staff or in accordance with the District's technology department's directives.

C. Electronic Communications with Students: Employees are prohibited from communicating with students who are enrolled in the District through electronic media, except as set forth herein. An employee is not subject to this prohibition to the extent the employee has a pre-existing social or family relationship with the student. For example, an employee may have a pre-existing 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. The following definitions apply for purposes of this administrative rule:

- "Authorized Personnel" includes classroom teachers, counselors, principals, associate ~~assistant~~ principals, Directors of Curriculum and Instruction and Pupil Services~~directors of instruction~~, coaches, ~~campus athletic coordinators,~~ athletic trainers, and any other employee designated in writing by the District Administrator or a building principal.

- "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. Unsolicited contact from a student through electronic means is not a communication.

- "Electronic media" includes all forms of social media, such as, but not limited by enumeration to, the following: text messaging, instant messaging, electronic mail (email), Web logs (blogs), electronic forums (chat rooms), video sharing Websites (e.g., YouTube™), editorial comments posted on the Internet, and social network sites (e.g., Facebook™, ~~MySpace™,~~ Twitter™, LinkedIn™), and all forms of telecommunication such as landlines, cell phones, and web-based applications.

D. Limited Electronic Communication with Students: Authorized ~~p~~Personnel may communicate through electronic media with students who are currently enrolled in the District only within the following guidelines:

1. The employee will ~~shall~~ limit communications to matters within the scope of the employee's professional responsibilities (e.g., for classroom teachers, items such as matters relating to class work, homework, and tests).

2. If an employee receives an unsolicited electronic contact from a student that is not within the employee's professional responsibilities (e.g., for classroom teachers, items such as matters relating to class work, homework, and tests), the employee will ~~shall~~ not respond to the student using any electronic media except to address a health or safety emergency.

3. The employee is prohibited from communicating with students through a personal social network page; the employee must create a separate social network page ("professional page") for this purpose. The employee must permit ~~enable~~ administration and parents to access the employee's professional page.

4. Only a teacher, coach, trainer, or other employee who has an extracurricular duty may communicate with students through text messaging. The employee may communicate only with students who participate in the extracurricular activity over which the employee has responsibility.

5. ~~The employee shall not communicate with any student between the hours of ____ p.m. and ____ a.m. unless the employee has supervisory responsibilities for the student at that time or to address a health or safety emergency. An employee may, however, make public posts to a social network site, blog, or similar application at any time.~~

6. Upon request from the 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.

E. Retention of Electronic Communications and other Electronic Media: The District archives all non-spam emails sent and~~/or~~ received on the system in accordance with the District's adopted record retention schedule. After the set time has elapsed, email communications may be discarded unless the records may be relevant to any pending litigation, pending public records request, or other good cause exists for retaining email records.

   Employees who create student records via email need to ensure that student records are retained for the period of time specified by the student records law. For this reason, the District heavily discourages the use of email as the means to communicate about individually identifiable students.

F. Electronic Recording: Employees shall not electronically record by audio, video, or other means, any conversations or meetings unless each and every person present has been notified and consents to being electronically recorded. Persons wishing to record a meeting must obtain consent from anyone arriving late to any such meeting. Employees must ~~shall~~ not electronically record telephone conversations unless all persons participating in the telephone conversation have consented to be electronically recorded. These provisions are not intended to limit or restrict electronic recording of publicly posted Board meetings, grievance hearings, ~~and~~ any other Board sanctioned meeting recorded in accordance with Board policy, and instruction. These provisions are not intended to limit or restrict electronic recordings involving authorized investigations conducted by District personnel, or authorized agents of the District, or electronic recordings that are authorized by the District, e.g. surveillance videos, extracurricular activities,

voicemail recordings).

G. Compliance with Laws and Local Policies and Regulations: For all electronic media, employees are subject to certain state and federal laws, local policies, and administrative regulations, even when communicating regarding personal and private matters, regardless of whether the employee is using private or public equipment, on or off District property. These restrictions include:
   1. Confidentiality of student records.

   2. Confidentiality of other District records, including educator evaluations, credit card numbers, and private email addresses.

   3. Confidentiality of health or personnel information concerning colleagues, unless disclosure serves lawful professional purposes or is required by law.

   4. Prohibition against harming others by knowingly making false statements about a colleague or the District.

   5. Prohibitions against soliciting or engaging in sexual conduct or a romantic relationship with a student.

   6. Upon written request from a parent or guardian, the employee shall discontinue communicating with the ~~parent's~~ minor student through email, text messaging, instant messaging, or any other form of one-to-one communication.

   7. An employee may request an exception from one or more of the limitations above by submitting a written request to the employee's~~his/her~~ immediate supervisor.

H. Personal Web Pages: Employees may not misrepresent the District by creating, or posting any content to, any personal or non-authorized website that purports to be an official/authorized website of the District. No employee may purport to speak on behalf of the District through any personal or other non-authorized website.

I. Personal Electronic Devices: The District permits staff to use personal technology devices in support of teaching and learning and to access the District's Wireless Public Network when doing so. Personal devices include laptop computers~~, portable digital assistants (PDAs)~~, cell phones, smart phones, iPads/tablets, iPods/MP3 players, wireless devices, digital cameras, e-readers, storage devices, or other electronics that may be carried on a person. Staff may use personal devices provided such use does not interfere with educational or employment responsibilities, hinder, disrupt, or consume an unreasonable amount of network or staff resources, or violate ~~b~~Board ~~p~~Policy, administrative rules, state law or federal law. An employee using a personal device must ~~shall~~ take adequate measures to ensure the confidentiality and proper maintenance of all student record information. The District is not liable for the loss, damage, or misuse of any personal device including while on District property or while attending school-sponsored activities.

J. Disclaimer: The District's electronic systems 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 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 systems are those of the individual or entity 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.