WASB 7/9/16

Verona Area School District **522.7-Rule**

STAFF RULES GOVERNING USE OF TECHNOLOGY, ELECTRONIC COMMUNICATIONS AND SOCIAL MEDIA

A. General

1. All employees are required to sign a "Technology Use Policy Agreement" form before they receive access to District technology systems.

2. The District's technology 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 technology systems, including electronic communication resources.

B. User Responsibilities

1. Users are responsible for the proper use of their individual accounts, and should take all reasonable precautions to prevent others from being able to use their personal accounts. Under no conditions should a user provide his/her password to another person. Users will immediately notify the site Educational Technology Coordinator if they have identified a possible security problem. Users will not search for security problems because this may be construed as an unauthorized attempt to gain access, i.e. computer hacking.

2. Users will be expected to use District technology systems in an appropriate manner. Users will not engage in any of the following conduct:

    a. Users may not use the District's technology systems for commercial purposes, including, but not limited to, purchasing, selling or advertising goods or services.
    b. Users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening or disrespectful language.
    c. Users will not post information that, if acted upon, could endanger the health, safety or welfare of other individuals.
    d. Users will not engage in personal attacks, including but not limited to, prejudicial or discriminatory attacks.
    e. Users will not harass or bully another person. "Harassment" refers to physical or verbal conduct, or psychological abuse, by any person that disrupts or interferes with a person's work performance, or which creates an intimidating, hostile or offensive working environment. If a user is told by a person to stop sending him/her messages, he/she must stop.

Staff must immediately disclose to their supervisor any electronic communications (e.g., messages) that are inappropriate or that make them feel uncomfortable.

f. Users will not engage in cyber bullying. "Cyber bullying" includes, but is not limited to the following misuses of technology: harassing, teasing, intimidating, threatening or terrorizing another person by sending or posting inappropriate and hurtful email messages, instant messages, text messages, digital pictures or images, or website postings that are materially or substantially disruptive or violate District policy. In situations in which the cyber bullying originated from a non-school computer or other communication device such as a cell phone and is brought to the attention of school officials, any disciplinary action taken shall be based upon whether the conduct is determined to be substantially disruptive of the work environment so that it markedly interrupts or substantially impedes the day-to-day operations of a school. In addition, such conduct must also be in violation of a publicized school policy. Such conduct includes, but is not limited to, harassment or making a threat off school grounds that is intended to endanger the health, safety or property of others at school or at a school-related activity wherever held, or toward a District employee or School Board member.
g. Users will not knowingly or recklessly post false or defamatory information about a person or organization.
h. Users will not use the District's technology systems to access or view material that is profane or obscene (i.e., pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature). If an employee inadvertently accesses or views such information, he/she should immediately disclose the inadvertent access in a manner specified by his/her supervisor. This will protect users against an allegation that they have intentionally violated District policy and rules. If a user receives inappropriate material through electronic transmission (e.g., email), he/she should notify the sender that such material is forbidden and should delete the material. If the sender continues to send such material, the user should notify his/her supervisor.
i. Users will not attempt to gain unauthorized access to the District's technology systems or to any other computer system through the District technology systems, or go beyond their authorized access. This includes attempting to log in through another person's account or access another person's files.
j. Users will not make deliberate attempts to disrupt the District's technology systems' performance or destroy data by intentionally spreading computer viruses or by any other means.
k. Users will not install software on a local hard drive nor will they download executable files without prior approval from the site Educational Technology Coordinator. Users will not alter any software configuration that is stored on a workstation. Users may download mobile Apps to a mobile device to preview for possible instructional use.
l. Users will not use the District's technology systems to engage in any illegal act or other action that violates any other District policy or rule.
m. Users will not access or disclose confidential student, personnel or other District record information without authorization. Any access to or disclosure of confidential student information must comply with state and federal laws governing the confidentiality of student records and the District's student records policy and guidelines.
n. Online gambling is strictly prohibited.

3. All users have access to a network drive and a Google cloud-based drive on which to store data. It is the responsibility of the user to practice file management, using network and/or cloud-based storage.

4. Users will respect the rights of copyright owners. Copyright infringement occurs when an individual inappropriately uses or reproduces a work that is protected by a copyright. If a work contains language that specifies acceptable use of that work, the user must follow the expressed requirements. If the user is unsure whether or not he/she can use a work, he/she should request permission from the copyright owner and appropriately reference it. District policies and guidelines on copyright govern the use of material accessed through District technology resources.

C. **Electronic Communications**

1. Electronic communications are protected by the same laws and policies and are subject to the same limitations as other types of district communications formats. The District expects staff to comply with state and federal laws and applicable District policies and guidelines when handling and working with student, personnel and District record information and data, including those dealing with the maintenance, confidentiality and retention of records. 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. Staff should be cautious when committing confidential information to electronic communications, as confidentiality cannot be guaranteed.

2. Because the District's technology systems, including all computer hardware, electronic communication devices and software, belong to the District, users have no privacy expectation in the contents of any of their personal files, including email, text messages and other forms of electronic communications, e.g. voicemail, Twitter™, Facebook™, etc. except as noted herein. Users also have no privacy expectation in any of the websites that they may visit by using the District's technology systems. Usage of the District's technology systems, including use of electronic communications, may be monitored without notice to determine compliance with the District's use of technology and electronic communications policy and rules. Through such monitoring process, the District may 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. If such personal Internet access information is obtained by the District, the District shall not use that access information to access the employee's personal Internet account unless permitted by law. Routine maintenance and monitoring may also lead to discovery that the user has or is violating the District's use of technology and electronic communications policy, rules or the law. An individual search will be conducted if there is a reasonable suspicion that a user has violated the law or District policy and/or rules. The search will be conducted consistent with legal requirements.

3. Retention of Electronic Communications: 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.

D. **Selection of Material for Class Activities**

1. When using the Internet for class activities, teachers will select age-appropriate material that is relevant to the course objectives. Teachers will preview the materials and sites they require or recommend students access to determine the appropriateness of the material contained on or accessed through the site. Teachers will provide guidelines and lists of resources to assist their

students in channeling their research activities effectively and properly. Teachers will assist their students in developing the skills to ascertain the truthfulness of information, distinguish fact from opinion, and engage in discussions about controversial issues while demonstrating tolerance and respect for those who hold divergent views. Teachers will instruct students in appropriate research and citation practices, and will instruct students to respect copyright and to request permission when appropriate.

2. Staff shall actively monitor students who are engaged in online learning activities to promote and develop good digital citizens.

E. **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 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 School Board meetings, grievance hearings, and any other Board-sanctioned meeting recorded in accordance with District policy. 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

F. **Use of Social Media**

1. Creating an Online Identity

a. Employees are responsible for their online/social media presence and are accountable for all written or posted materials, whether posts are through a District-sponsored account or a personal account. Employees must use sound judgment at all times and adhere to applicable guidelines found in the District's Social Media Handbook. The permeating and permanent effect of social networking cannot be overstated.
b. Employees have no expectation of privacy when using social media sites/online forums. Information posted on or exchanged through social media may be accessed by parents, students, co-workers, and members of the public. Therefore, when communicating via online social media, it is important for employees to remember that their conduct represents the District and any information posted or exchanged should always be in the best interests of serving the District and its students.
c. Employees may not misrepresent the District by creating or posting any content to any personal or non-authorized social media account that purports to be an official District-sponsored social media account. No employee may purport to speak on behalf of the District through any personal or other non-authorized social media account.
d. District information posted to a social media personal profile must be limited, but may include District employment information including District name, job title and duties, status updates on job promotion, and personal participation in District-sponsored events, including volunteer activities.
e. When making personal, non-work-related posts online, employees will not use their District email addresses in the message or for reply purposes as they may inadvertently and inappropriately imply approval of the message's content by the District.

2. Online Conduct

District employees must comply with provisions of the District Use of Social Media policy when using District-sponsored social media accounts and any other standards or rules that have been established including, but not limited to the following:

a. District employees will not use social media accounts to harass, threaten, libel, malign, defame, disparage or discriminate against members of the school community, including but not limited to students, parents and/or guardians, co-workers or the administration, or the School Board.

b. District employees may not reference personally identifiable information concerning District students in any way on social media sites except as specifically authorized by District policy (e.g., the posting of student photos on District-sponsored social media sites under established conditions) or specifically approved by the employee's supervisor.

c. District employees must avoid communicating with families and students regarding school or District-related matters through personal social media accounts, blogs, etc.

d. District employees may not post photos of other staff on District-sponsored social media accounts without their consent.

e. Non-public images of the District premises and property, including floor plans, or other proprietary or confidential information of the District may not be posted on or communicated via social media accounts.

f. Communications with Students: District employees shall limit communications with students through social media accounts to matters within the scope of the employee's professional responsibilities (e.g., for classroom teachers, matters relating to class work, homework, and tests; and for coaches, trainers, or other employees with extracurricular duties, matters pertaining to the activity.) An employee is not subject to this limitation to the extent the employee has a family or social relationship with the student (e.g., niece or nephew, child of an adult friend, student is a friend of the employee's child, babysitter, member or participant in the same civic, recreational, or religious organization). Staff shall not link to or accept students as "friends" on personal social media accounts such as LinkedIn, Facebook or other similar accounts/sites.

3. Compliance with Applicable Laws and Policies

District employees remain subject to applicable state and federal laws, other District policies and administrative rules, and Employee Handbook provisions when using social media, including but not limited to:

- Prohibitions against discrimination (Board Policies 411 and 511)
- Prohibitions against harassment (Board Policy 512)
- Prohibitions against bullying, including cyber bullying (Board Policy 443.8)
- Confidentiality of student records (Board Policy 347 and related administrative guidelines)
- Confidentiality of personnel records (Board Policy 526)
- Access to Public Records (Board Policy 823 and related administrative procedures)
- Communications provisions in the Employee Handbook (Part I – Section 3.06)
- Student-Staff Relations provisions in the Employee Handbook (Part I - Section 3.29)

G. **Use of Personally-Owned Laptops and Other Computing or Communications Devices at School**

1. A personally-owned laptop computer, handheld computer or other computing or communications device may be connected to the Internet at school only through the District's public wireless network, which allows filtered web-only access to the Internet. Connecting a laptop or other device to a non-networked device such as a projector or Smartboard is allowed for instructional purposes.

2. The laptop computer, handheld computer, or other computing or communications device is to be used in compliance with District policies and rules, including but not necessarily limited to those applicable to the use of District technology and electronic communications. Any violation of such policies or rules may result in the exclusion of the device from school and/or discipline of the person who has violated the policy and/or rule.

3. Personally-owned devices will not be able to access district printers or copiers.

4. If a personally-owned technology device (e.g., cell phone) is found, or is confiscated, the person recovering the device is not authorized to view the contents of the device. District protocol requires staff to place the device in a clear ziplock bag (depending upon the size of the device), label it with the time/date, and turn it in to the office. The district administrative staff or agent and/or a law enforcement representative are the only one authorized to view the contents, and any search or review of the contents of the device must be consistent with legal requirements.

5. The District may examine personally-owned computers and other communications devices and search their contents if there is a reason to believe that school policies, rules or regulations or laws have been violated. The scope of the search will be limited to the violation of which the employee is accused, and the search will be conducted in a manner consistent with legal requirements. Individuals have no expectation of privacy in the use of the District's wireless network or technology systems and such use is subject to being monitored.

6. Employees are not required to bring personally-owned laptop computers or other communications devices to school. The District accepts no responsibility for the loss, theft or damage of personal property brought to school by employees. Any laptop computer, handheld computer, or other communications device is the responsibility of the staff member who brought the device to school.

H. **Policy and Rule Violations**

1. The District will cooperate fully with local, state or federal officials in any investigation concerning or relating to any illegal activities conducted through the District's technology systems.

2. Employee violations of the District's use of technology and electronic communications policy and/or rules shall be handled in accordance with applicable District policies and provisions of the Employee Handbook.

APPROVED IN PART: August 31, 2015

REVISED: August 15, 2016