WASB 7/9/16

Verona Area School District **363.2-Rule**

STUDENT INTERNET SAFETY/APPROPRIATE USE OF TECHNOLOGY RULES

A. **General**

1. The District's technology resources, including District-owned mobile devices, software, networks and network connections, are open to regulated use by students as a privilege. Each student who uses the District's technology resources is required to follow the District's established expectations for appropriate use.

2. Students should approach their use of technology resources with the understanding that all of the school rules and expectations that apply to in-person interactions and to the student's general conduct while at school or while under the supervision of a school authority also apply to their use of District technology, their online conduct, and their electronic communications. This rule and various other District policies, rules and regulations include additional requirements and expectations that are directly related to the use of technology resources, including District-owned mobile devices. If a student has a question concerning any policy, rule, regulation or directive that relates to technology resources, or if a student encounters a situation in which they are uncertain about any expectation for appropriate use or about how to proceed, the student should contact a teacher or an administrator to obtain appropriate guidance.

3. Because the District's technology resources belong to the District, users have no privacy expectation in the contents of any of their personal files, including but not limited to email and other electronic communications, on the District's technology resources. Users also have no privacy expectation in any of the websites that they may visit by using the District's technology resources. Usage of the District's technology resources may be monitored without notice to determine compliance with the District's Internet safety and appropriate use policy and rules. Through such monitoring process, the District may inadvertently obtain access information for a student'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 student's personal Internet account unless permitted by law. Routine maintenance and monitoring of the District's technology resources may also lead to discovery that the user has or is violating the District's 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 the District's Internet safety and appropriate use policy and/or rules. The search will be conducted consistent with legal requirements.

4. The District makes no guarantees of any kind, either expressed or implied that the functions of the services provided by or through the District technology resources will be error free or without defect. The District will not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service. The District is not responsible for the accuracy or quality of the information obtained through or stored on the system. The District will not be responsible for financial obligations arising through the unauthorized use of the District's technology resources.

B. **Parental Role and Responsibilities**

1. Upon consultation with the site administrator, and consistent with rules governing the confidentiality of student records, parents/guardians may investigate the contents of their children's technology use files upon request.

2. There is a wide range of material available on the Internet, some of which may not fit with a particular family's values. Although the District has an Internet filtering measure in place, it is impossible to ensure complete protection from access to inappropriate material. It is not possible for the District to monitor and enforce a wide range of social values in student use of the Internet. Further, the District recognizes that parents/guardians bear primary responsibility for transmitting their particular set of family values to their children. The District will encourage parents/guardians to specify to their children what material is and is not acceptable for their children to access through the District's technology resources.

C. **Appropriate Use Rules**

1. Personal Safety
   a. Students will not post personal contact information about themselves or other people on the Internet. Personal contact information includes, but is not limited to, home address and telephone number. Exceptions may be made for career or post-secondary educational research purposes, or with approval by an instructor.
   b. Students will not agree to meet with someone they have met online without their parent'(s)/guardian'(s) approval and participation.
   c. Students must immediately disclose to their teacher or other staff members present any electronic communications (e.g., messages) they receive that are inappropriate or that make them feel uncomfortable.

2. Social Networking
   a. Web resources that emphasize collaboration and sharing, such as online chat rooms, wikis, blogs, forums and other Web 2.0 tools, may be used for educational or school-related purposes as determined by District instructional or administrative staff. All other use of social networking sites and resources by students is prohibited.

3. Unauthorized Activities
   a. Students may not use the District’s technology resources for commercial purposes, including, but not limited to, purchasing, selling or advertising goods or services.
   b. Students will not attempt to gain unauthorized access to the District’s technology resources or to any other computer system through the District’s technology resources, or go beyond their authorized access. This includes attempting to log in through another person's account or access another person's files.
   c. There shall be no downloading or installing of programs or applications on to District technology resources, including District-owned mobile devices, without teacher permission. Students are not allowed to load personal software on to District technology resources, including a District-owned mobile device, at any time.
   d. Students will not make deliberate attempts to disrupt the District’s technology resources’ performance or destroy data by intentionally spreading computer viruses or by any other means.
   e. Students will not use the District’s technology resources to engage in any illegal act or other action that violates any other District policy or rule.

f. Mobile devices come with a standardized image already loaded. Any other image set as the desktop background or screensaver must be in line with District policies and rules. Inappropriate media may not be used, which includes any presence of guns, weapons, pornographic materials, inappropriate language, alcohol, drugs, or gang-related symbols.
g. Mobile devices come equipped with special functions such as a webcam. Webcams are to be used for educational purposes only, under the direction of the teacher. Listening to music or watching movies on the device is not allowed during school hours without permission from the teacher. Permission will be given only for media used to complete a school project or assignment. Students may be permitted to listen to music or watch a movie on a District-owned mobile device during non-instructional time and off school premises.
h. Online gaming, music downloads and streaming and video downloads and streaming is not allowed on District technology equipment, including District-owned mobile devices, except with teacher permission and only if such activity is in support of education, as determined by instructional staff. Online gambling is strictly prohibited.

4. System Security and Data Management
   a. Students are responsible for the use of their individual accounts and should take all reasonable precautions to prevent others from being able to use their personal accounts. Students may only log in to their assigned mobile device or District network under their assigned username. Students may not share their log-in and password with other students or individuals. Students may share their log-in and password with their parents/guardians.
   b. Students will immediately notify the site Educational Technology Coordinator if they have identified a possible security problem. Students will not search for security problems because this may be construed as an unauthorized attempt to gain access, i.e. computer hacking.
   c. All students have access to a network drive and a Google cloud-based drive on which to store data. It is the responsibility of the student to manage their files, saving as needed to either the network drive or Google cloud.

5. Cyber Bullying/Respect for Privacy
   a. Students will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening or disrespectful language. Restrictions against inappropriate language apply to public messages, private messages and material posted on websites.
   b. Students will not post information that, if acted upon, could endanger the health, safety or welfare of other individuals.
   c. Students will not engage in personal attacks, including but not limited to, prejudicial or discriminatory attacks.
   d. Students 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 student’s school performance, or which creates an intimidating, hostile or offensive learning environment. If a user is told by a person to stop sending him/her messages, he/she must stop.
   e. Students 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 educational process 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.

f. Students will not knowingly or recklessly post false or defamatory information about a person or organization.

6. Plagiarism and Copyright Infringement
   a. Students will not plagiarize. Plagiarism is taking the works of others and presenting them as if they were original to the user. District policies on plagiarism will govern use of material accessed through District technology resources.
   b. Students will respect the rights of copyright owners. Copyright infringement occurs when an individual inappropriately 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 on copyright govern the use of material accessed through District technology resources.

7. Inappropriate Access to Material
   a. Students will not use the District's technology resources 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).
   b. If a student inadvertently accesses or views such information, he/she should immediately disclose the inadvertent access in a manner specified by his/her teacher. This will protect users against an allegation that they have intentionally violated District policy and rules.
   c. If a student receives inappropriate material through electronic transmission (e.g., email), the student should notify the sender that such material is forbidden and should delete the material. If the sender continues to send such material, the student should notify his/her teacher or site administrator.

D. **Personally-Owned Laptops and Other Computing or Communications Devices**

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 Internet safety and appropriate use of District technology resources. 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. Any student who brings a laptop computer, handheld computer or other computing device to school must use it as an instructional tool and only for the school curriculum. It may not be used as an entertainment system. Students must turn off and put away a personally-owned laptop, handheld computer or other computing device when directed by a staff person.

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

5. 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.

6. 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 student 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.

7. Students 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 students. Any laptop computer, handheld computer, or other communications device is the responsibility of the student who brought the device to school.

E. **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 technology resources.

2. In the event there is an allegation that a student has violated the District Internet Safety and Appropriate use policy and/or rules, staff will investigate and meet with the appropriate individuals. The student will be given an opportunity to be heard in the manner set forth in the building disciplinary codes. Disciplinary actions are tailored to meet specific concerns related to the violation and to assist the student in gaining the self-discipline necessary to behave appropriately on an electronic network. Consequences of violations of the Internet safety and acceptable use policy and rules include but are not limited to:

   · Suspension of network privileges
   · Revocation of network privileges
   · Suspension of Internet privileges
   · Revocation of Internet privileges
   · School suspension and/or expulsion
   · Legal action and prosecution by the authorities
   · Other disciplinary action

APPROVED: July 21, 1997

REVISED: June 2, 2002
April 7, 2003
May 17, 2010
August 15, 2016