DISTRICT ACCEPTABLE USE /INTERNET SAFETY RULES

A. Purpose

1. The District provides employees and students with access to the District's technology systems, which includes the VASD Bulletin Board (an on-line space to list classified ads, excluding the promotion of commercial/personal businesses), the District's Internet, intranet, e-mail, telephone, computer equipment and computer systems (collectively referred to as the "Systems"). Access to the Systems by employees, students and others requires adherence to the District's policy (the "Policy"), other District policies and state and federal laws and regulations.

2. The primary purpose of providing access to the Systems is to enhance teaching and learning, thereby better preparing students for success in life and work. This access is provided to increase communication within the District, enhance productivity and assist users in improving their skills. Access is also provided to assist in the sharing of information with the local community, including parents/guardians, social service agencies, government agencies and businesses.

3. The Systems are to be used for school-related administrative and educational purposes. However, limited personal use of the Systems is permitted during non-instructional or non-supervisory time. Excessive personal use of the Systems may result in disciplinary action.

4. The e-mail system may not be used for commercial purposes, including, but not limited to purchasing, selling, or advertising goods or services. Non-commercial classified listings must be made on the VASD Bulletin Board. Fundraising efforts that support the school or school-sponsored activities may be posted on site/activity websites with the building principal's approval.

5. District employees must recognize that electronic files and communications may be public records subject to state open records requirements, and they must take appropriate actions to maintain such records in compliance with state law.

6. The District makes no guarantees of any kind, either expressed or implied that the functions of the services provided by or through the Systems 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 system.

B. Responsibilities Related to Technology System Management and Training

1. The District's Director of Technology works with the site Educational Technology Coordinators and Network Manager to manage, maintain and improve the Systems.

2. The site Educational Technology Coordinator serves as the building level coordinator for the Systems, and ensures staff and students receive proper training in the use of the Systems and the requirements of this Policy and other applicable rules.

3. Internet safety instruction will be delivered to students by staff as outlined in the District's Internet Safety Curriculum.

4. Staff will actively monitor students who are engaged in online learning activities.

5. Staff at grades K-3 must preview Web sites for student access prior to use.

6. The District shall maintain an Internet filtering measure that blocks access to the three categories of visual depictions specified by the Children's Internet Protection Act - obscene material, child pornography and material that is deemed harmful to minors. The District's Internet filtering measure may be relaxed or disabled for bona fide research or other lawful purposes.

C. Access to the System

1. This Policy, including but not limited to Section F below, provides the primary guidance for use of the Systems by students and staff. All students and staff will be given the opportunity to access the network.

2. District staff must sign a "Network User Agreement" form before access is provided.

3. Students must abide by the rules outlined in Section F below, Acceptable Use Rules, which are also referenced in the student handbook.

4. A guest may receive an individual account with the approval of the site Educational Technology Coordinator or the building principal if there is a specific, District-related/District-approved purpose requiring such access. Use of the Systems by a guest must be specifically limited to District-approved purposes.

D. Parental Notification and Responsibility

1. The District will notify parents/guardians about the Systems and the policies and rules governing their use. This Policy will be available on the District website.

2. 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.

3. 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 systems.

E. Selection of Material

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.

F. Acceptable 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, address, telephone and work address. 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. Staff must immediately disclose to their supervisor any messages they received that are inappropriate or that make them feel uncomfortable.

d. Students must immediately disclose to their teacher or other staff members present any messages they receive that are inappropriate or that make them feel uncomfortable.

2. Social Networking

a. The use of online social networking sites such as chat rooms, wikis, blogs, forums and other Web. 2.0 tools will be allowed only in controlled, staff-supervised settings, and for valid school-related purposes. All other uses are prohibited.

b. Staff shall not post any information regarding students on Internet sites that were not created for school-related activities. Staff may create/participate in group sites that support school-approved activities.

c. Staff shall not link to or accept students as “friends” on personal Internet sites such as LinkdIn and Facebook or other similar sites.

3. Unauthorized Activities

a. Users will not attempt to gain unauthorized access to the Systems or to any other computer system through the Systems, or go beyond their authorized access. This includes attempting to log in through another person's account or access another person's files.

b. Users will not install software on the 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.

c. 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.

d. Users will not use the District system to engage in any illegal act or other action that violates any other Board Policy.

e. Online game playing, music downloads and streaming, video downloads and streaming and online gambling, unless used to gather educational materials for classroom instruction, is strictly prohibited.

4. System Security

a. Users 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. Under no conditions should a user provide his/her password to another person.

b. 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.

5. Cyber Bullying/Respect for Privacy

a. Restrictions against inappropriate language apply to public messages, private messages and material posted on Web pages.

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" is defined as persistently acting in a manner that distresses or annoys another person. If a user is told by a person to stop sending him/her messages, he/she must stop.

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 video, or Web site postings that are materially or substantially disruptive or violate Board 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. 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.

6. Respecting Resource Limits

a. The Systems are to be used for educational and professional development activities. To promote an equitable sharing of resources, users may not monopolize or abuse access to the Systems by, among other possibilities, storing an excessive amount of information or using the Systems for unauthorized purposes such as listening to the radio or watching video clips outside the context of a school-related activity. Users are encouraged to check their email frequently and delete unwanted messages promptly. Further, users need to practice file management in home and/or shared folders.

7. Plagiarism and Copyright Infringement

a. Users 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 the Systems. Teachers will instruct student in appropriate research and citation practices.

b. Users 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 using the Systems. Staff will instruct students to respect copyright and to request permission when appropriate.

c. Downloading and/or sharing of files, images, music, or video without obtaining the permission of a teacher or administrator is prohibited.

8. Inappropriate Access to Material

a. Users will not use the Systems, including use of personally owned computers with the 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).

b. If a user inadvertently accesses or views such information, he/she shall immediately disclose the inadvertent access in a manner specified by his/her teacher or supervisor. This will protect users against an allegation that they have intentionally violated this Policy.

c. If a Systems user receives inappropriate material by email, said user should notify the sender that such material is forbidden and should delete that material. If the sender continues to send such material, the user should notify his/her supervisor.

G. District, School and Classroom Web Sites

1. The District Web site is maintained by District Office Staff.

2. Each school has a Web site that is updated by site staff, under the direction of the site Principal and Educational Technology Coordinator**.**

3. Staff may have a classroom Web site that they may utilize to post announcements, resources, assignments and activities.

4. Training will be provided as needed to assist staff in managing their Web pages.

5. When creating Web pages, staff should keep in mind that the published pages will be viewed by a worldwide audience. These guidelines should be followed when creating content for any and all District, school and classroom Web pages. By doing so, the District hopes to insure the integrity of the information and the safety of all staff and students.

    a. All policies regarding use of the Systems are applicable to Web pages.

    b. Photos of class activities and students are allowed consistent with the Family Educational Rights and Privacy Act (FERPA). At the elementary and middle school level, only student first names may be associated with the photo. At the high school level both first and last names may be used.

    c. Elementary and middle school staff should not include students' last names with specific pieces of work. This includes names within the content of student work. Student work may be posted on Web pages.

    d. All material posted must adhere to copyright laws. (Contact the site Educational Technology Coordinator or Library Media Center Director with questions regarding “Fair Use”.)

e. Pages should not be used to display commercial advertisements or solicitations other than for fundraising for District-sponsored events and activities as approved by the building principal.

f. Links to other Web sites from pages should be fully investigated to make sure that the content, including advertisements on pages, is appropriate for students.

g. The author(s) of the pages is responsible for maintaining them, i.e., keeping the content current and links active.

h. Annually, in September, staff will receive notification of names of students whose parents/guardians have filed a written notice requesting their child/children's picture(s) or works not appear on Web pages. Coaches, club/activity supervisors and others who wish to post student photos or works are responsible for obtaining this information from the site office and for compliance with this policy.

H. Monitoring, Search and Seizure

1. System users (Staff, students and guests) have no privacy expectation in the contents of any of their files, including, but not limited to e-mail and voicemail files, on the Systems.

2. System users also have no privacy expectation in any of the websites that they may visit by using the Systems. Usage of the Systems may be monitored without notice to determine compliance with this policy.

3. Routine maintenance and monitoring of the systems may lead to discovery that the user has or is violating the District's Internet safety and acceptable use policy, rules or the law.

4. 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 acceptable use policy and/or rules.

5. District employees are reminded that materials stored on their computers including their personal files may be discoverable and subject to release under state public open records laws.

I. 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 only through the District’s public wireless network, which allows filtered web-only access to the Internet. Connecting a laptop to a non-networked device such as a projector or Smartboard is allowed for instructional purposes only.

2. The laptop computer, handheld computer, or other computing or communications device is to be used in compliance with District policies and rules. Users will be bound by all policies and rules. Users will be bound by all policies and rules of the District applicable to the use of the Systems. 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 staff or student who brings a laptop computer, handheld computer or other computing/communication 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 personal laptop, handheld computer or other computing device when directed by a staff member.

4. If a cellphone is found or is confiscated the person recovering the phone is not authorized to view contents on the phone. District protocol requires staff to place the phone in a clear ziplock bag, label it with 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.

5. The District may examine personal computers and other electronic devices and search their contents if there is a reason to believe that school policies, including this policy, rules or regulations or laws have been violated. Individuals have no expectation of privacy in the use of the District's wireless network or Systems and such use is subject to being monitored.

6. Neither students nor staff are required to bring personal electronic property to school. The District accepts no responsibility for the loss, theft or damage of personal property brought to school by staff or students. Any laptop computer, handheld computer, or other electronic device is the sole responsibility of the staff member or student who brought the device to school.

J. 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 Systems.

2. In the event there is an allegation that a user has violated the District Internet safety and Acceptable Use Policy and/or rules, an investigation will be conducted and the user will be afforded due process rights. Students will be given an opportunity to be heard in the manner set forth in student disciplinary codes. Student 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 measures

3. Employee violations of the District's Internet safety and acceptable use policy and/or rules shall be handled in accordance with applicable District policies and applicable collective bargaining agreements.

4. A guest user's account may be terminated at any time with or without notice.

APPROVED: July 21, 1997

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