POLICY # 3202: CURRICULUM (CONTINUED)

3202.8 COMPUTER NETWORK AND INTERNET ACCEPTABLE USE

Definition of Terms: ***The Oceanside School District computer network*** *refers to the interconnection of computers, servers and other electronic devices within a classroom, school, or district which facilitates file sharing, resource sharing, communication, collaboration, management, and access to remote resources.* ***The Internet*** *is a decentralized network of computer networks which provides connectivity to commercial, educational, organization and government resources and facilitates local and global communication.* ***Internet filtering*** *is a method by which information that is available on the Internet but is deemed inappropriate for children is made unavailable for general viewing.* ***Vandalism*** *is defined as any malicious attempt to harm or destroy district equipment or materials, data of another user of the district's network, or of any of the entities or other networks that are connected to the Internet. This includes, but is not limited to, creating and/or placing a computer virus on the network.*

Philosophy: It is our district's philosophy that access to technological resources is an integral part of the curriculum and the instructional process. At the same time, there is an inherent responsibility on the part of users to conduct themselves in an appropriate and considerate manner when using this medium. Although electronic materials are selected for their educational value and Internet resources are filtered for inappropriate content, the security, accuracy and quality of information that is available through our network cannot be guaranteed. The guidelines that follow have been developed to inform students, teachers and parents/guardians about the expectations that are associated with the responsible use of our computer network and the Internet. It is ultimately the responsibility of families to set standards and for students to be responsible for their own behavior.

Instructional Services: Students and teachers have access to a wide variety of electronic resources through our Local Area Network, including curriculum software, multimedia CD-ROMs, computer servers, and library automation systems. Through our Wide Area Network, students also have access to external electronic resources that are not controlled by the District such as Internet e-mail, which enables communication with peers and experts throughout the world, and the World Wide Web, which facilitates the exploration of thousands of databases, libraries, universities, government agencies, museums and commercial sites. These services are currently available in libraries, computer laboratories, and classrooms under the supervision of teaching staff and/or instructional assistants who provide supervision, training, and support to all users.

POLICY # 3202: CURRICULUM (CONTINUED)

3202.8 COMPUTER NETWORK AND INTERNET ACCEPTABLE USE (CONTINUED)

Parent/Guardian Responsibilities: Parents/Guardians should review this Acceptable Use Policy with their children and return the agreement form to school. This agreement form will be sent home prior to entrance into third, seventh, and ninth grades as well as to all new entrants. A signature indicates agreement that these resources will be used responsibly, fairly, and appropriately by the child. Completed agreement forms will be retained in students' Cumulative Record folders.

Acceptable Use: The following guidelines have been established for acceptable use of the Oceanside Public Schools computer network and Internet access. **Users should be aware that the District reserves the right to ensure compliance through electronic monitoring of network and Internet usage.** Users shall have access to the Internet through our network as long as they follow the provisions of this policy.

1. While all students and staff are welcome to use our network, priority will be given to those individuals who are using it for curriculum-driven and for research-oriented purposes.

2. The use of our network,WiFi and equipment is a privilege to be used responsibly, fairly and appropriately. The same behavioral expectations of students and staff while in school, and the community apply to online behavior.

3. District-owned equipment and software should be treated with care and should not be vandalized, damaged, stolen, or abused in any way.

4. Users should be polite and courteous while online and may not use insulting, vulgar, or demeaning language or create or post or provide access to inappropriate visual material. While users have a right to express their ideas, they are also responsible for the content they create, transmit or publish, including e-mail, posted messages, file and web pages.

5. Users may not publish new web pages or modify existing web pages without the authorization of a staff member, designated by the District Director of Technology.

POLICY # 3202: CURRICULUM (CONTINUED)

3202.8 COMPUTER NETWORK AND INTERNET ACCEPTABLE USE (CONTINUED)

Acceptable Use (continued)

6. Users may not access private accounts or subscribe to mailing lists, bulletin boards, chat groups or commercial services without the authorization of a staff member designated by the District Director of Technology.

7. The use of the network to purchase personal items or services is prohibited.

8. Attempts should not be made to gain access to unauthorized systems, breach security passwords, or log on in the name of another individual.

9. Attempts should not be made to circumvent our filter to access inappropriate Internet content. A designated staff member should be contacted if a user needs to access a blocked web site.

10. Do not reveal personal addresses, phone numbers or other confidential information

11. Users who "log-on" with a username and password shall "log-off" when not at the computer. This will disallow other users from accessing their accounts or having access to user rights to which they would normally not have access.

12. Employing district-owned hardware for commercial activities, product advertising, political lobbying or any other activities that are not directly related to an approved educational or job-related use is prohibited. This activity can significantly degrade the bandwidth available for other users engaged in educational pursuits.

POLICY # 3202: CURRICULUM (CONTINUED)

3202.8 COMPUTER NETWORK AND INTERNET ACCEPTABLE USE (CONTINUED)

Acceptable Use (continued)

13. The use of district-owned technology resources for personal use while on the District network is prohibited. Examples of personal usage include, but are not limited to, shopping, banking, employing Internet radio sites, personal printing, computer games, videos, streaming media and browsing auction sites. These activities often significantly degrade the bandwidth available for our first priority; that is educational purposes. The District does not object to reasonable and occasional personal usage when taking place outside of the regular school day and hence, not competing with an educational need for bandwidth. Personal usage should not be a regular practice and those who abuse this privilege may have their personal use denied. Guidelines relating to personal usage are in place to ensure staff and students have the best possible bandwidth for educational uses.

14. Installing, downloading, changing, or modifying software or software setups without prior consent of the technology department is prohibited.

Remote access: Users accessing the Oceanside UFSD Infrastructure remotely shall use devices approved by the District. Remote access to the Oceanside UFSD Infrastructure must use identification, authentication, and encryption techniques to safeguard all internal District computer systems. All remote access must be approved and shall be restricted to those individuals with a specific purpose to access the internal network remotely. Remote access users shall be given the least access privileges necessary to carry out their job-related functions. All remote access users may be given a security orientation to minimize security risks to the District. Methods of network access shall be explored to include VPN access through the firewall.

POLICY # 3202: CURRICULUM (CONTINUED)

3202.8 COMPUTER NETWORK AND INTERNET ACCEPTABLE USE (CONTINUED)

Acceptable Use for Vendors:

All Vendor access to Oceanside UFSD's Infrastructure must be approved. Access to the Oceanside UFSD's Information Infrastructure shall be restricted to the lowest security level necessary to accomplish Vendors' tasks. All Vendors for the Oceanside UFSD Infrastructure shall agree to abide by the District's Policies. Upon acceptance of a contract with the District, Vendors shall agree to access and use the Oceanside UFSD Infrastructure responsibly according to this policy and in accordance with their Vendor role. Vendors shall be held legally responsible for misuse of their access and use of the Oceanside UFSD Infrastructure. Vendors may have their Oceanside UFSD network activity monitored by the District. Oceanside UFSD shall make every reasonable effort to ensure that reputable companies are used for outsourcing of computer processing. Vendors shall not remotely access the Oceanside UFSD Infrastructure without the prior express permission of the District. Access is generally granted by the Information Technology Department in the form of computer and network accounts granted to users and others, as appropriate, for such purposes as vendor support or contracted development. Vendors will not attempt to disguise their identity, or the identity of their account. Vendors will not attempt to impersonate other persons or organizations. Vendors will not appropriate Oceanside UFSD's name, or its network names. Vendors will not attempt to monitor other users' data communications unless specifically authorized. Vendors will not infringe upon the privacy of others' computer files. Vendors will not read, copy, change, or delete another user's computer files or software without the prior express permission of the owner. Vendors shall not engage in actions that interfere with the use by others of any computers and networks, interfere with the supervisory or accounting functions of the systems, or are likely to have such effects. Such conduct includes, but is not limited to, placing of unlawful information on the system, transmitting data or programs likely to result in the loss of the recipient's work or system downtime, or any other use that causes congestion of the networks or interferes with the work of others. Vendors will not attempt to bypass computer or network security mechanisms without the prior express permission of the Information Technology Department. Possession of tools that bypass security or probe security, or of files that may be used as input or output for such tools, shall be considered as the equivalent of such an attempt. Vendors who require remote access to the Oceanside UFSD's network will be required to have virus protection software program installed. This program must be operational and be using the latest virus detecting upgrades for computers used for this purpose.

POLICY # 3202: CURRICULUM (CONTINUED)

3202.8 COMPUTER NETWORK AND INTERNET ACCEPTABLE USE (CONTINUED)

Supervision and Monitoring: It shall be the responsibility of all professional employees (pedagogical and administrative staff) to supervise and monitor usage of the School District's computers, computer network and access to the Internet in accordance with this policy, the Acceptable Use Policies, and the Children's Internet Protection Act. Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Director of Technology or designated representatives.

Education: The District will advocate and educate employees, students, parents and the Oceanside community on Internet safety and "cyber-bullying". Education will be provided through such means as professional development training and materials to employees, PTA presentations, and community outreach opportunities such as School District websites.

Designated representatives will provide age appropriate training for students who use the District's Internet facilities. The training provided will be designed to promote Oceanside's commitment to student safety, appropriate behavior while online, on social networking Web sites, and in chat rooms; and cyber-bullying awareness and response.

Social Networking Sites (SNS) for District Employees:

The School District recognizes the value of teacher and professional staff inquiry, investigation and communication using new technology tools to enhance student learning experiences. The School District also realizes its obligations to teach and ensure responsible and safe use of these new technologies. Social media, including social networking sites, have great potential to connect people around the globe and enhance communication. Therefore, the Board of Education encourages the use of District-approved social media tools and the exploration of new and emerging technologies to supplement the range of communication and educational services.

POLICY # 3202: CURRICULUM (CONTINUED)

3202.8 COMPUTER NETWORK AND INTERNET ACCEPTABLE USE (CONTINUED)

Social Networking Sites (SNS) for District Employees: (continued)

For purposes of the Policy, the definition of public social media networks or Social Networking Sites (SNS) are defined to include: Web sites, Web logs (blogs), wikis, social networks, online forums, virtual worlds, video sites and any other social media generally available to the school district community which do not fall within the District's electronic technology network (e.g., Facebook, MySpace, Twitter, LinkedIn, Flickr, Vine, Instagram, Snap Chat, blog sites, etc.). The definition of District-approved password-protected social media tools are those that fall within the District's electronic technology network or which the District has approved for educational use. Within these internal forums, the District has greater authority and ability to protect minors from inappropriate content and can limit public access within these internal forums.

The use of social media (whether public or internal) can generally be defined as Official District Use, Professional/Instructional Use, and Personal Use. The definitions, uses and responsibilities will be further defined and differentiated in the Administrative Regulation. The School District takes no position on an employee's decision to participate in the use of these media during District time or on District-owned equipment is discouraged. In addition, employees are encouraged to maintain the highest levels of professionalism when communicating, whether using District devices or their own personal devices, in their professional capacity as educators. The have responsibility for addressing inappropriate behavior or activity on these networks, including requirements for mandated reporting and compliance with all applicable District Policies and Regulations.

POLICY # 3202: CURRICULUM (CONTINUED)

3202.8 COMPUTER NETWORK AND INTERNET ACCEPTABLE USE (CONTINUED)

Ethical and Legal Considerations: Use of our computer network must conform to district policies and local, state and federal laws. The following are prohibited:

1. Use of our network to access, store, distribute or promote illegal activities such as, but not limited to, bomb-making, drugs, gambling or pornography.

2. Use of our network to promote violence, racism, sexism, or other forms of discrimination.

3. Use of our network to install, use, store, duplicate or distribute copyrighted materials, including software, files, video clips, photographs, graphics, text, music, or speeches.

4. Use of our network to plagiarize the work of others.

5. Use of our network for non-school related promotion of political candidates or causes.

6. Use of our network for commercial advertisements or profit-making purposes.

Personal Security Issues: Users, particularly students, should follow these guidelines to maintain ongoing access to our network and to ensure their personal security:

1. Information that is sent or received over our network is subject to review.

2. Users should exercise common sense and discretion when sending **or receiving electronic information (e.g. e-mail) over our network since it is public in nature and has no guarantee of privacy.**

POLICY # 3202: CURRICULUM (CONTINUED)

3202.8 COMPUTER NETWORK AND INTERNET ACCEPTABLE USE (CONTINUED)

Personal Security Issues (continued)

3. Users should never distribute personal information such as names, addresses, telephone numbers, credit card numbers, social security numbers, bank accounts, PIN numbers or photographs.

4. Users should never make appointments to meet people in person whom they have contacted online without written authorization from a designated staff member, parent/guardian, and/or supervisor.

5. Users should notify a staff member whenever they come across information or messages that are dangerous, illegal, obscene and inappropriate or make them feel uncomfortable**.**

District Employee Responsibilities: It is the responsibility of staff members to help implement this policy by taking the following steps:

1. Inform all students of the existence of the district policy before making the network available to students.

2. Take appropriate disciplinary actions when students violate any aspect of this policy.

3. Report serious policy violations to an administrator.

4. Respond immediately to student notification of dangerous, illegal, obscene, or inappropriate information transmitted over our computer network and report it to an administrator.

POLICY # 3202: CURRICULUM (CONTINUED)

3202.8 COMPUTER NETWORK AND INTERNET ACCEPTABLE USE (CONTINUED)

Confidentiality, Private Information and Privacy Rights: for District Employees

Access to confidential data is a privilege afforded to District employees in the performance of their duties. Safeguarding this data is a District responsibility that the Board of Education takes very seriously. Confidential and/or private data, including but not limited to, protected student records, employee personal identifying information, and District assessment data, shall only be loaded, stored or transferred to District-owned devices which have encryption and/or password protection. This restriction, designed to ensure data security, encompasses all computers and devices, any mobile devices, including flash or key drives, and any devices that access the network from remote locations.

Staff will not leave any devices unattended with confidential information visible. All devices are required to be locked down while the staff member steps away from the device, and settings enabled to freeze and lock after a set period of inactivity. Staff data files and electronic storage areas shall remain District property, subject to District control and inspection.

Staff use of the District's computer network and Internet access is conditioned upon electronic, annual acknowledgment by the staff member.

Consequences of Violations: The consequences for violating this policy will be consistent with the District's Discipline Policy and may include the following:

1. Temporary suspension of access to the computer network and the Internet.
2. Notification of school authorities.
3. Notification of parent/guardian.
4. Permanent suspension of access to the computer network and the Internet.
5. Financial restitution.
6. Legal action.

(Revised 7/1/16) (Revised 4/23/01) (Adopted 4/19/01)