4-12 Student Technology Acceptable Use Policy

(A) Purpose

Technology provides exciting opportunities to expand learning for students and educators. However, with this opportunity comes the responsibility for appropriate use. The intent of the Okaloosa County School District's Technology Acceptable Use Policy is to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254 (h)]. Therefore, the School Board of Okaloosa County has adopted the following Student Technology Acceptable Use Policy to guide students as they access and use the electronic resources in Okaloosa County Schools.

(B) Overview

The internet will be accessible to all Okaloosa County Schools through the Okaloosa County Schools Network and through various other access providers. The Okaloosa County Schools Network has not been established as a public access service or as a public forum. Therefore, the School Board has the right to place reasonable restrictions on the material accessed or posted through the system. Users are also expected to follow the rules set forth in the Code of Student Conduct and the law in their use of the internet. Our goal in providing internet access to faculty, staff and students is to promote educational excellence in Okaloosa County Schools by facilitating resource sharing, innovation and communication.

There may be some material or individual communications which are not suitable for school-aged children. The School Board firmly believes that the valuable information and interaction available on this worldwide network far outweighs the possibility the users may obtain material inconsistent with the educational goals of the District.

The District views information gathered from the internet in the same manner as reference materials identified by the schools. Specifically, the District supports resources that will enhance the learning environment while providing directed guidance and monitoring from school faculty and staff. While it is impossible to control all material on a public network, the District has taken reasonable precautions to restrict access to materials it considers harmful, and to materials that do not support approved educational objectives

(C) Educational Purposes

This policy pertains to all technology devices, including but not limited to: computers (laptop, desktop), BYODs (Bring Your Own Devices), cell phones, smart devices, tablets; regardless if the device is property of the student or District.

(1) Technology access is a privilege and not a right. All students will have access under school supervision to Internet World Wide Web information resources through their classroom, media center or school technology lab.

(2) The user and his/her parents must sign the District's MIS Form 5251 before being granted access to the OCSD network or the internet through a school's electronic resources. Computer access can be withdrawn from a student at any time by either a member of the school's staff or the student's parents/guardians.

(3) All student web pages created as part of a school project must relate to the specific school, educational and/or career informational activities and have a teacher sponsor.

(4) As in the case of school lockers and other physical storage areas, electronic storage devices and/or areas are subject to inspection at any time. School administrators, either directly or through support, may view files and communications to ensure system integrity and to be sure that users are using the system responsibly. Users should not expect that files stored on District technology are private. All outgoing transmissions of information are unsecured and sent at the risk of the user.

(5) The District cannot assure the rights of privacy on its computer systems. Parents/Guardians have the right at any time to request to see the content of their student's computer files.

(6) Individual users of technology are expected to follow the generally accepted rules of network etiquette.

(D) Procedural Guidelines

(1) The District will remove any information from the system that school staff determines to be unlawful, obscene, pornographic, abusive, harassing or otherwise in violation of this policy, including all items deemed as harmful matter. School staff will refer for disciplinary actions any individual who violates provisions of this policy. Cancellation of user privileges and other consequences will be at the discretion of the school principal or designee.

(2) Vandalism of a District computer system will result in cancellation of privileges and/or disciplinary action that may include notification of law enforcement. Vandalism includes, but is not limited to: the uploading or creation of computer viruses or similar software, the hacking or altering of software and physical damage to electronic hardware. Parents/Guardians may be held financially responsible for any harm resulting from their student's misuse of the computer system.

(3) Purposeful access, downloading or transmission of any harmful matter in violation of any federal law, state law or district policy is prohibited. This includes, but is not limited to:

(a) Any information that violates or infringes upon the rights of any other person

(b) Any hate-motivated, fraudulent, defamatory, abusive, obscene, profane, sexually-oriented, threatening, harassing, bullying, racially offensive or illegal language or material

(c) Any information or communication that encourages the illegal use of controlled substances or promotes criminal behavior

(d) Any material that violates copyright laws

(4) All electronic resources are to be used in a responsible, efficient, ethical and legal manner. Users must acknowledge their understanding of this policy as a condition of using technology resources. Acceptable uses of the internet are activities that support learning, collaborative work and teaching.

(E) Unacceptable Uses

(1) Attempting any unauthorized access to any computer system is illegal and will be treated as such. Unacceptable uses of the internet include, but are not limited to the following:

(a) Violating the condition of the Student Code of Conduct, especially those dealing with students' rights to privacy.
(b) Downloading inappropriate materials for personal use (e.g. files, graphics, music and/or movies).
(c) Re-posting personal communications without the author's prior consent.
(d) Videotaping and rebroadcasting images, videos, etc. without consent of the subject.
(e) Copying commercial software in violation of copyright law or other copyright protected materials, including photographs.
(f) Installing or storing any software on any District computer without the permission of the teacher or staff member responsible for the computer.
(g) Making or attempting to make any changes in any configuration, password or program on any computer system without permission.
(h) Using any District computer without permission of the teacher or staff member responsible for that computer.
(i) Use of vulgarities or any other inappropriate language, pictures or gestures on the internet in any form, including written, graphic, voice phone, and real-time.
(j) Playing unauthorized online games or accessing unauthorized social media.
(k) Damaging computers, computer systems, software, computer networks or data belonging to the District or someone else.
(l) Any attempt to disrupt technology or network function.
(m) Using another person's user ID or password.
(n) Revealing the full name, personal address, social security number or telephone number of any student, school staff member or district employee.
(o) Use of District computers to access personal email should be limited to educational purposes only and requires teacher or administrative approval.
(p) Monitoring network traffic for personal information
(q) Attempting to gain access to other users' usernames and passwords for any reason.
(r) Remote access of other networks, computers, servers or other technology without permission from teacher or administrator.

(2) Taking or storing inappropriate images or video. Any violation of this policy that is also a violation of federal or state laws may also result in criminal prosecution.

(F) Mobile Devices

(1) Mobile Device Rules of Acceptable Use:

(a) Unless you have been expressly permitted by the instructor to use your mobile device or applications on your mobile device for a classroom task, students agree not to:
    (1) Have their mobile devices out or on (regular school/district policy applies)
    (2) Text
    (3) Make calls
    (4) Play games
    (5) Turn on Bluetooth
    (6) Take pictures or video
    (7) Utilize any other applications not mentioned above

(b) Students agree to abide by their mobile device plans (discussed with parents). Students will not access mobile web. On days that the mobile devices are used in class, students will have their mobile devices out on their work area in full view. Students agree to abide by any school specific rules for mobile devices.

(c) The consequences for violating the Mobile Device Rules of Acceptable Use may be, but are not limited to the following:

(1) The first time a student violates the Mobile Device Rules of Acceptable Use, the student will lose privileges of participation in the classroom digital activities for one (1) week. His/her mobile device will be confiscated for the remainder of the class period by the teacher.

(2) The second time a student violates the Mobile Device Rules of Acceptable Use; the student will lose privileges of participation in the classroom digital activities for two (2) weeks. His/her mobile device will be confiscated and turned into the office. This may result in an office referral.

(3) The third time a student violates the Mobile Device Rules of Acceptable use; the student will lose the privilege of using the mobile device at school. The mobile device will be confiscated and turned into the office and will result in an office referral.

(G) Smart Devices and Testing

Smart devices, to include but not limited to cell phones, smart watches, tablets, some calculators, may be prohibited from being used/worn during a testing environment. Teachers/administrators should have a secure place to store such devices.

(H) Limitation of Liability

The School Board makes no warranties of any kind, whether expressed or implied, for the service it is providing. The School Board will not be responsible for any damages a user may suffer, including loss of data. The School Board will not be responsible for the accuracy or quality of information obtained through any District internet connection. Parents will indemnify the District against any damage that is caused by the student's inappropriate use of the system.

(I) Computer Virus Protection

(1) Users must avoid knowingly or inadvertently spreading computer viruses.
    (a) Do not download files from unknown sources.

(b) Always download files to a computer that has adequate virus detection and protection installed.
(c) Deliberate attempts to degrade or disrupt system performance will be viewed as criminal activity under applicable state and/or federal law.
(d) Schools should scan all storage media for viruses before being used on district computers.
(e) Do not connect any computer or electronic device to the internet unless it has been approved by District Seat Management Project Manager, Dustin Keith.

(J) Access to Inappropriate Material

To the extent that is practical, technology protection measures (or "internet filters") shall be used to block or filter internet, or other forms of electronic communication, access to inappropriate information. Specifically, as required by the Children's Internet Protection Act (CIPA), blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to staff supervision, technology protection measures may be disabled for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes.

(K) Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the District online computer network when utilizing electronic mail, social media, instant messaging, and other forms of direct electronic communications. Specifically, as required by CIPA, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called "hacking," and other unlawful activities; and (b) unauthorized disclosure, use and/or dissemination of personal identification information regarding minors.

(L) Education, Supervision and Monitoring

(1) It shall be the responsibility of all members of the District staff, including but not limited to site based instructional personnel, to educate, supervise and monitor appropriate usage of the online computer network and access to the internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.
(2) The District, independently or through contracted technology vendors, has the right to remotely monitor network traffic and computer workstations for the purpose of maintaining the security of the network, troubleshooting computer repair, and assisting with technology related problems.
(3) Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Superintendent or designated representatives.
(4) Schools will provide age appropriate training for students who use their internet facilities. The training provided will be designed to promote the District's commitment to:
   (a) The standards and acceptable use of internet services as put forth in the Technology Acceptable Use Policy.
   (b) Student safety with regard to:

(1) Safety on the internet
(2) Appropriate behavior while online, on social media websites
(3) Cyberbullying awareness and response

(c) Compliance with the E-rate requirements of the Children's Internet Protection Act.

Following receipt of this training, the student will acknowledge that he/she received the training, understood it and will follow the provisions of the District's Student Technology Acceptable Use Policy.

Statutory Authority: Sections 1001.41(2); 1001.42, Florida Statutes

Laws Implemented: Section 1001.43(3)(A), Florida Statutes; 47 USC 254(h); Public Law No. 106-554

Adopted: November ___, 2015