



Title: **Student Technology and Internet Acceptable Use Policy**

Code: 04-12

Section: Chapter 04 - Students

04-12 STUDENT TECHNOLOGY AND INTERNET 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 and Internet 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 and Internet 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. 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.

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, Chromebook), BYODs ("Bring Your Own Devices"), cell phones, smart devices, smart glasses, including prescription smart glasses, and tablets; regardless if the device is property of the student or District. This policy also outlines the use and access of the internet provided by the School District.

- (1) Technology access is a privilege and not a right. All students will have access under school supervision and after District content filtering, 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 District 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) The District will protect the safety and security of students when using email, chat rooms, and other forms of direct electronic communication. This is done by:
 - (a) Limiting student email communication to other District email addresses only; and
 - (b) Restricting available chat rooms to District-managed Learning Management Systems; and
 - (c) Using the Firewall or Internet Filter to block unregulated chat rooms, email, or other communications tools.
- (7) Students are restricted from accessing websites, web applications, or software, which require student personally identifiable information (PII) to be provided by the student, without permission of the teacher or the school's administration, after confirmation that a Student Data Privacy Agreement, through the District, is in place which protects such PII from unauthorized disclosure, use, or dissemination.

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 provisions 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. Taking or storing inappropriate images or video.
 - (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.
 - (k) Accessing data, Information, or activities (including hacking) considered unlawful
 - (l) Accessing social media platforms through the use of District provided internet access, except when expressly directed by a teacher solely for educational purposes.
 - (m) Viewing or using TikTok, or any of its successor platform services on District-owned devices, through Internet access provided by the District. TikTok, or any successor platforms, may not be used to communicate with or promote any school, school-sponsored club, extracurricular organization or athletic team.
 - (n) Damaging computers, computer systems, software, computer networks or data belonging to the District or someone else.
 - (o) Any attempt to disrupt technology or network function.
 - (p) Using another person's usernames or passwords.
 - (q) Revealing the full name, personal address, social security number or telephone number of any student, school staff member or district employee.
 - (r) Use of District computers to access personal email should be limited to educational purposes only and requires teacher or administrative approval.
 - (s) Monitoring network traffic for personal information
 - (t) Remote access of other networks, computers, servers or other technology without permission from teacher or administrator.
 - (u) Attempting to gain access to other users' usernames and passwords for any reason.
 - (v) Taking, recording, or storing unauthorized or inappropriate images or video.
 - (w) "Sexting" at any time on school property or at school functions. As set forth in Florida law, sexting is the knowing transmission or distribution to another minor by a computer or similar device any photograph or video of any person that depicts nudity and is harmful to minors. Sexting also includes possessing a photo of any person that was transmitted or distributed by another minor that depicts nudity. Such conduct is not only potentially dangerous for the involved students, but can lead to unwanted exposure of the messages and images to others, and could result in criminal violations related to the transmission or possession of child pornography. Such conduct will be subject to discipline and possible confiscation of the wireless communications device(s).
- (2) The consequences for violating the Student Technology Acceptable Use Policy can be found in the Code of Student Conduct. Any violation of this policy that is also a violation of federal or state law may result in criminal prosecution.

(1) Wireless Communications Device Rules of Acceptable Use:

- (a) In accordance with the provisions of Florida Law, a student may be in possession of wireless communications devices while he or she is on school property or in attendance at a school function. Unless otherwise provided by this policy such devices must be turned off and securely stored on silent during the school day. For the purposes of this policy, wireless communications devices, or mobile devices, include cellular telephones, electronic tablets, e-readers, smart glasses, including prescription smart glasses, or other similar wireless communications devices, however, for purposes of this policy, a student may not possess smart glasses, including prescription smart glasses, on School Board property or on school district transportation, or while attending a school function unless expressly authorized by §1006.07(2)(f)(2), *Florida Statutes*.
- (b) Elementary and middle school students may not use a personal wireless communications device during the school day unless it is needed to monitor a health condition, to accommodate a disability or in a designated location within the school building as expressly authorized by the school principal. Appropriate documentation shall be provided to the school prior to authorization of any such use by the school principal.
- (c) Medical alert devices must be registered with the school health clinic. For students with disabilities, assistive devices must be approved in the student's IEP, 504 Plan or individual school health plan. Misuse of these devices may result in disciplinary action.
- (d) Unless permitted by the high school instructor, a school administrator or authorized in a student's IEP or 504 Plan, students, during the school day, including while off-campus on a field trip and at school sponsored events shall not:
 - (i) Have their mobile devices out (regular school/district policy applies)
 - (ii) Text
 - (iii) Make calls
 - (iv) Play games
 - (v) Turn on Bluetooth
 - (vi) Take pictures or video
 - (vii) Utilize any other applications not mentioned above
- (e) High School students using their personal mobile devices in a classroom setting shall access online capabilities through the District network only. All students are prohibited from using any recording device, including but not limited to wireless communications devices, cameras, audio recorders, or other electronic or mechanical equipment to capture, record or transmit words (i.e. audio) and/or images (i.e., pictures or video) of any student, staff member or other person in the school or while attending a school-related activity during the school day, without express prior notice to such individual(s) and explicit consent from the school principal or his/her designee for the capture, recording or transmission of such words or images. Using a wireless communications device or any other electronic, mechanical or other recording device to take or transmit audio and/or pictures/video of an individual without his/her consent is considered an invasion of privacy and is not permitted.
- (f) Wireless communications devices, including but not limited to those with cameras, may not be activated or utilized at any time in any school situation where a reasonable expectation of personal privacy exists. These locations and circumstances include, but are not limited to locker rooms, shower facilities, restrooms/bathrooms, and any other areas where students or others may change clothes or be in any stage or degree of disrobing or changing clothes. The Superintendent and school principals are authorized to determine other specific locations and situations where use of a device is absolutely prohibited.
- (g) Students shall have no expectation of confidentiality with respect to their use of wireless communications devices on school property or at District sponsored events.
- (h) Students are prohibited from using wireless communications devices in any way that might reasonably create in the mind of another person an impression of being threatened, humiliated, harassed, embarrassed, or intimidated.
- (i) Students are prohibited from using wireless communications devices to capture and/or transmit test information or any other information in a manner constituting fraud, theft,

cheating, or academic dishonesty. Likewise, students are prohibited from using wireless communications devices to receive such information.

- (j) High School teachers shall designate an area in the classroom for the secure storage of wireless communication devices during instructional time.
- (k) Notwithstanding any provisions of this policy to the contrary, while on District transportation students may, subject to the acceptable use provisions of this policy, use their personal mobile devices for non-disruptive activities such as completing school work, reading, privately listening to music with earphones or ear buds, texting or playing games. Students are prohibited from using wireless communications devices to capture, record or transmit words (i. e. audio) and/or images (i.e., pictures or video) of any student, staff member or other person while on District transportation, without express prior notice to such individual(s) and explicit consent from the bus driver for the capture, recording or transmission of such words or images. Using a wireless communications device to take or transmit audio and/or pictures/video of an individual without his/her consent is considered an invasion of privacy and is not permitted. The proper use of personal mobile devices is under the direction of the bus driver and/or bus assistant. Failure of a student to comply with directions given by the bus driver and/or bus assistant may result in disciplinary consequences as set forth in this policy.
- (l) The consequences for violating this Wireless Communications Devices policy can be found in the Code of Student Conduct. Any violation of this policy that is also a violation of federal or state laws may result in criminal prosecution.

(G) Smart Devices and Testing

Smart devices, including but not limited to cell phones, smart watches, tablets, and 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's Seat Management Specialist.

(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 his/her designee.
- (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 this Student Technology and Internet Acceptable Use Policy.
 - (b) Student safety with regard to:
 - (i) Safety on the internet
 - (ii) Appropriate behavior while online
 - (iii) For students in grades 6-12, the social, emotional, and physical effects of social media
 - (iv) Cyberbullying awareness and response
 - (c) Compliance with the e-Rate requirements of the Children's Internet Protection Act.

By signing MIS form 5251 Student Technology and Internet Acceptable Use Policy, the student and their parent/guardian will acknowledge that they received, reviewed, and understood the District's Student Technology and Internet Acceptable Use Policy, and will follow all the provisions of the policy. This policy should be signed at enrollment and again annually.

Adopted: **October 23, 2000**

Last Revised: **May 26, 2026**

Last Reviewed: **October 14, 2024**

Prior Revised Dates: **November 13, 2007; November 9, 2016; July 31, 2018; July 24, 2023; July 28, 2025**

Additional Resources

Statutory Authority: §§1001.41(2) and 1001.42(28), *Florida Statutes*

Laws Implemented: §§934.03, 1001.43(3)(A), 1003.02(1), 1003.32(1), 1003.42(2), and 1006.07, *Florida Statutes*; 47 USC 254(h); Public Law No. 106-554
