POLICY 6633
STUDENT TECHNOLOGY ACCEPTABLE USE POLICY

The Kenosha Unified School District expects students to use technology in ways that promote a productive educational environment. Technology includes, but is not limited to, electronic devices, private and public networks, and electronic communication systems managed within KUSD. These may include common technologies utilizing the Internet, Wi-Fi, laptops, iPads, and other related tools available to staff and students. With this educational opportunity comes personal responsibility. Primary responsibility for appropriate use of technology resources resides with the student. School and network administrators and staff will review files and communications to maintain system integrity and to ensure that the network is used responsibly. All communication including text and media files may be disclosed to third parties and/or law enforcement without prior consent of the sender or receiver.

In accordance with requirements of the Children's Internet Protection Act (CIPA), technology protection measures shall be used, to the extent practical, to promote the safety and security of users. Access to inappropriate electronic material and communications will be filtered. Digital Media and mobile devices are dynamic and continue to increase in functionality with enriched usage by students and staff. Allowing students the opportunity to utilize their own devices within district technology networks and staff monitored environments will only expand the skillset needed to operate in a comfortable and responsible manner. Student-owned devices should only be used as a resource for learning, and strengthen the integration with curriculum and collaboration. Aligned with the Protecting Children in the 21st Century Act, KUSD will continue to reinforce the instructional practices related to Internet safety, appropriate online behavior, social networking, chat rooms, and cyberbullying issues. Review and agreement of this policy is an annual expectation for students and parents/guardians.

LEGAL REF.: Wisconsin Statutes
Sections 120.12(1) [School Board duties]
120.13 [School Board powers]
943.70 [Computer crimes]
947.0125 [Unlawful use of computerized communication systems]
U.S.C. 17, Federal Copyright Law [Use of copyrighted materials]
Children's Internet Protection Act [Online safety]
Neighborhood Children's Internet Protection Act [Online safety]
Children's Online Privacy Act [Online privacy protection]
Broadband Data Improvement Act, Title II, Section 215 [Internet safe use]
Protecting Children in the 21st Century Act

CROSS REF.: 3531.1, Copyrighted Materials
3535, Technology Acceptable Use
5111, Anti-Bullying/Harassment/Hate
5430, Student Conduct and Discipline
5437, Threats/Assaults
6120, Core Values
6470, Student Records
6600, Instructional Resources
6610, Selection of Instructional Materials
6620, Library Resources
6634, Assistive Technology

AFFIRMED: November 28, 1995

REVISED: January 29, 2002
May 22, 2007
July 28, 2009
June 28, 2011
June 25, 2013
March 22, 2016

RULE 6633
STUDENT TECHNOLOGY ACCEPTABLE USE POLICY

General school rules for behavior and communications apply, including the District's anti-harassment policies. Students shall abide by District guidelines governing Internet safety and acceptable use of technology. Misuse of electronic resources including the Internet may result in loss of access privileges and school disciplinary action may be taken. Appropriate legal action may also be taken against students performing illegal activities using electronic resources.

- Students shall not engage in any electronic activity that disrupts, distracts, or compromises the learning process or the environment.
- Electronic activities must not contain profanity, obscene comments, sexually explicit material, or expressions of bigotry, racism, or hate**,** or be disorderly.
- Students shall not use District technology resources for personal commercial activities not related to instruction. Personal purchase or sale of products or services is prohibited.
- Students shall have the ability to use their own devices within communicated instructional guidelines and practices while on school grounds.
- Students must abide by all applicable copyright and licensing laws when using technology resources within the District.
- Students shall maintain confidentiality of their usernames and passwords and shall not utilize usernames and passwords of others.
- All school related electronic publications are subject to approval and ongoing review by staff. All publications should reflect the mission and cores values of the school and District.
- Students shall not breach or disable network security mechanisms or compromise network stability or security in any way. Student**s** shall refrain from utilizing proxy gateways to bypass monitoring or filtering.
- Students are responsible for reporting any inappropriate media or resources they encounter**,** regardless of who owns the device.
- Students shall not use any technology or communication system for any other purpose that would violate law or Board policy (including harassment policies).

The District's technology resources are District assets. While the District respects the privacy and security needs of all individuals, authorized District representatives may review, audit, intercept, access and/or disclose all communications created, received or sent using District technology.

Use of Personally Owned Technology Equipment Connected to District Network Infrastructure
1. Personal technology may be used to connect to the District infrastructure, when authorized.
2. The use of personal technology must not interfere with legitimate educational purposes and must be used in accordance with the overall Technology Acceptable Use Policy.
3. Personal technology devices and applications must not interfere with the operation and integrity of the District's internal wired and wireless network.
4. The District is not responsible for the support, safety, or security of personal technology devices that students choose to bring into the District.

Electronic information, including the Internet, is dynamic. This makes it challenging to predict or reliably control what information students may encounter. District staff makes every reasonable effort to filter inappropriate content.