Approved 1/11/2021

SCHOOL BOARD POLICY **FILE: 363**
School District of Holmen **SECTION: 300**
Holmen, WI 54636 **INSTRUCTION**

ACCEPTABLE USE POLICY (AUP)

Philosophical Foundation:

The School District of Holmen (District) recognizes that information technology resources significantly impact the operational and instructional environment of our district. Additionally, the District supports access to information and technology resources by District stakeholders (students, staff, community, parents, guests, etc.) and strives to ensure that the use of technology is efficient, safe, and appropriate.

The District recognizes that its technology systems are provided through public funding and, as such, every effort is made to allow public access to School District of Holmen's network where possible and where such access does not negatively impact operations of the District.

This policy aligns with the guidelines for the Children's Internet Protection Act (CIPA) and the Neighborhood Children's Internet Protection Act (NCIPA) and The Broadband Data Improvement Act. To that extent practical steps shall be taken to promote the safety and security of the users of the School District of Holmen. Students and staff will receive information and updates about acceptable use of technology annually.

As members of a global economy, use of technology brings responsibilities as well as opportunities. The Board expects that students will benefit from the integration of information technology throughout the curriculum. District staff will provide guidance and instruction to students in the appropriate use of this technology as well as support related to cyber-bullying awareness and response.

Therefore, the Board of Education (Board) directs that the accompanying guidelines establish expectations for staff and student conduct and behavior with regard to the use of technology.

Agreement to Terms Herein

This policy applies to users of District technology, District networks and District technology systems. It additionally applies to users of personal technology within the District or at District-sponsored events.

All district policies and student handbook guidelines are applicable in determining acceptable or unacceptable use of technology.

Internet Safety

Students will be provided developmentally appropriate guidance as they make use of technology and electronic communication systems to conduct research and other studies related to the District curriculum. Students will be informed of their rights and responsibilities as users of technology prior to gaining access.

Although the District has an Internet filtering measure in place, it is impossible to ensure complete protection from access to material that some may find objectionable. Further, the District recognizes that parents/guardians bear the primary responsibility for communicating their particular set of values in this regard to their children. The District encourages parents/guardians to specify to their children what material is and is not acceptable for them to access via District systems.

The District shares responsibility with parents and community regarding access to Internet sites and technology resources. Partnerships with parents and community shall help address Internet safety and appropriate use of Internet resources.

The District reserves the right to block sites that do not enhance classroom activities. The District will make due efforts to ensure filtering meets requirements of the Children's Internet Protection Act to provide protection from obscene, pornographic and other materials considered harmful to minors. Staff may request access to blocked sites when they believe such access has curricular merit.

If a user inadvertently accesses or views inappropriate information, they shall immediately disclose the inadvertent access in a manner specified by their teacher or supervisor. This will protect users against an allegation that they have intentionally violated this policy.

If a user receives inappropriate material by any means, 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 their teacher or supervisor.

Responsibility for Information Accessed, Obtained, or Lost

The School District of Holmen makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District does not warrant that the functions of its systems will meet any nor that such systems will be error-free, nor that their operation be uninterrupted.

The District will not be liable for any direct, indirect, incidental, or consequential damages (including lost data, information, or use time) sustained or incurred in connection with the use, operation, or inability to use District technology systems. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

Students and staff should have no expectation of privacy with regard to the use of the District's technology systems.

Nothing residing in a student's technology device, files, District email or other District-managed electronic communication system will be deemed personal, private or confidential.

All electronic communications transmitted by, received from or stored in the District's network are owned by the District. The District may access, search, monitor and/or disclose to appropriate authorities any communication at any time without prior notice.

The District may monitor user activities on its technology systems.

Personally Owned Technology

Personally owned technology must be used in accordance with this policy. "Personally-owned technology" includes, though is not limited to wearable technology, such as a smart watch.

The following additional terms apply to using personally-owned technology in the District or at a District-sponsored function.

1. Personally owned technology may be connected to the District's network only through the District's publicly accessible wireless network.
2. Students must turn off and put away personal technology when directed by a staff member.
3. If technology is found or confiscated the person recovering the device may not be authorized to view the contents of the device. District students and staff shall immediately provide the building administration or law enforcement with the device as they are the only ones authorized to view the contents.
4. The District may examine personal technology and search their contents if there is reason to believe that school policies, rules, regulations, or laws may have been violated.

5. The District accepts no responsibility for the loss, theft, or damage of personal property brought to school by staff or students.
6. Users may not install District software onto personal devices unless software is explicitly licensed for such use.
7. Any violation of policies or rules may result in the exclusion of the device from school, exclusion of the device from District's networks and/or discipline of the person found to be in violation.

Social Media

All of the District's policies, rules and procedures apply to online conduct, including engagement in social media.

The following guidelines shall be followed in relation to student and staff use of social media:

1. Staff will use social media resources for the sole purpose of meaningful learning.
2. The use of social media and other online tools will be allowed only in a controlled, teacher supervised, setting and for valid instructional purposes consistent with the educational objectives of the School District of Holmen.
3. Transmission of any material in violation of any national, state, or District regulation or policy is prohibited. This includes, but is not limited to, copyrighted, harassing, threatening, or obscene material.
4. Students will not post information that, if acted upon, could endanger the health, safety, or welfare of other individuals.
5. Students should understand that what they post online on different media venues is public. They need to understand their digital footprint is for all to see. Students should understand that they should not post anything they would not want their friends, parents, grandparents, teachers, or a future employer to see.
6. When students disagree with someone else's opinion, they should respond constructively and respectfully. What is inappropriate in the classroom is inappropriate online.
7. Be safe online. Never give out personal information, including but not limited to: Last names, phone numbers, addresses, birthdate, and pictures.
8. Before publically supporting a website or article, make sure that you read it in its entirety.
9. Do not misrepresent yourself by using someone else's identity.
10. Staff shall not "friend", connect or otherwise interact with current students on social media platforms using the staff member's personal social media account(s).

Account-Based Services

Staff may choose to utilize online resources, cloud-based services and social networking platforms for instruction and communication with District stakeholders.

District staff may allow students to create "accounts" approved by the District when necessary for using cloud-based services, accessing resources, sharing information, turning in assignments, or communicating with teachers (for example). These accounts will be created in full compliance with the Children's Online Privacy Protection Act (COPPA). All usage agreements, including age restrictions, will be followed. If a staff member wishes to have students under the age of 13 access online resources that are restricted by age, procedures to inform parents of the accounts will be used.

Staff-to-Student Electronic Communication

District-approved communication systems must be used for electronic communications from a staff member to student(s) and groups of students. Approved communication systems include District email. A current full list of approved communication systems can be obtained from the District's I&T department.

Prohibited Activities

The following activities are not permitted and may result in an investigation and potential disciplinary actions:

1. Using obscene or inappropriate language or content.
2. Engaging in cyberbullying. Cyberbullying is defined as "willful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices."
3. Sending or posting cruel or threatening messages or images.
4. Downloading, displaying, viewing, accessing or attempting to access, storing or transmitting any images, messages or material which may be construed as threatening, harassing, offensive or to others based upon gender, race, national origin, age, disability, religion, sexual orientation or any other basis protected by applicable law.
5. Unreasonable personal use, or personal use that interferes with the employee's or other District user's performance of his/her duties, or which otherwise disrupts the operations of the District.
6. Using technology and/or communication systems for commercial or political purposes
7. Use which is illegal, including the violation of copyright, defamation, gambling and pornography laws.
8. Damaging any component of the District's computer hardware or software.
9. Occupying excessive file storage space on District servers.
10. Unauthorized accessing or attempting to access confidential District information, including but not limited to personnel records, medical records and financial information pertaining to the District or any of its employees or students.
11. Unauthorized accessing or attempting to access another employee's or student's password, data, messages or other electronic communication's materials (Statute 943.70).
12. Posting private information about the student or any other person, including but not limited to addresses, telephone numbers, identification numbers, account numbers, passwords or access codes.
13. Re-posting a message that was sent to the user without permission of the person who sent the message.
14. Pretending to be someone else and sending or posting material that makes that person look bad or places that person in potential danger.
15. Electronic activities must not contain profanity, obscene comments, sexually explicit material, or expressions of bigotry, racism, or hate, or be disorderly in nature or cause another to be disturbed or distracted.
16. Wastefully using information technology resources, including but not limited to printing.
17. Sharing account information with others including passwords.
18. Failing to protect confidential information.
19. Accessing or viewing material that is profane or obscene (i.e. pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature).
20. Any use that is inconsistent with the school's Code of Conduct.
21. Use of personal email for District business.

Violations

Violations of this policy may result in suspension of technology privileges, termination of technology privileges and/or other disciplinary action. The level of discipline will vary based on the severity of the violation, the harm caused and other relevant factors. When applicable, law enforcement agencies may be involved.

Disciplinary action may be determined at the building level in line with existing practice regarding inappropriate language or behavior.

District reserves the right to discipline a student for actions taken off-campus if such actions are intended to have an effect on a student or adversely affect the safety or well-being of a student while in school.

District reserves the right to discipline a student for actions taken off-campus if they are intended to impact the District's technology systems, whether such systems are housed within the District or in cloud computing environments outside of the District.

Parents, guardians or adult students wishing to appeal decisions related to the denial of student access to technology resources may appeal in writing to the building administrator.

Legal Reference:	Wisconsin State Statutes Sections: 120.13 (1) School government rules 943.70 Computer Crimes 947.0125 Unlawful use of computerized systems 118.258 Electronic communication devices prohibited PL 94-553, Federal Copyright Law, PL 110-395, Broadband Data Improvement Act of 2008 (Title II Protecting Children in the 21st Century) Children's Internet Protection Act (CIPA) Children's Online Privacy Protection Act (COPPA) Neighborhood Children's Internet Protection Act (NCIPA)
Cross Ref.:	411, Equal Education Opportunity 511, Equal Employment Opportunity 443, Student Code of Conduct 443.7, Anti-Bullying Policy 446, Student Searches & Seizures 361, Instructional & Media Resources Selection, Reconsideration and Withdrawal 443.10, Technology Access for Students with Special Needs 724, Information & Technology Systems Security 771.1, Use of Copyrighted Materials Employee Handbook

Adopted:	October 25, 1999
Revised	August 19, 2002
Approved:	September 9, 2002
Revised:	February 11, 2008
Approved:	May 27, 2009
Revised:	May, 2010
Approved:	June 14, 2010
Revised:	February 18, 2013
Approved:	March 11, 2013
Revised:	October 12, 2015
Approved:	November 23, 2015

Revised: November 16, 2020
Approved: January 11, 2021