

ACCEPTABLE USE POLICY (AUP)

Philosophical Foundation:

The School District of Holmen 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 school stakeholders (students, staff, community, parents, guests, etc.) and strives to ensure that the use of technology is efficient, safe, and appropriate.

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.

Providing access to technology resources (software and hardware) is an important part of preparing District students for today's world. This goal includes the following objectives:

- Students and staff will use information and technology ethically and responsibly;
- Students and staff will be provided e-mail services for school-related activities to improve communication skills;
- Students will be engaged learners when they are provided with relevant learning activities;
- Students will benefit from more timely and targeted assessment and feedback;
- Students will benefit from differentiated instruction that is technological enhanced;
- Students and staff will be provided equitable access to technology resources
- The students will gain skills that will mirror the world of college and career
-

As members of a global economy, use of information technology and communication resources and systems 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 directs that the accompanying guidelines establish expectations for staff and student conduct and behavior with regard to the use of networked information resources.

- Leg Ref.: Wisconsin Statutes
 Sections 120.13 (1) Board duty; care and control of school district property
 943.70 Computer Crimes
 947.0125 Unlawful use of computerized systems
 118.258
 121.01(1)(h) Instructional Materials
 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.: Equal Education Opportunity, 411
 Equal Employment Opportunity, 511
 Student Code of Conduct, 443
 Anti-Bullying, 443.7
 Guidelines for Student Search & Seizure, 446
 Employee Code of Conduct, 522
 Employee Relations Handbook

Instructional & Media Resources Selection, Reconsideration and Withdrawal, 361
Technology Access for Students with Special Needs, 443.10
Bullying & Intimidation, 443.11
Copyright, 771.1
Guidelines for Student Search and Seizure, 446

Adopted: October 25, 1999
Rev/App: August 19, 2002/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

Continued on next page...

Internet Safety

Students will be provided developmentally appropriate guidance as they make use of technology and communication resources to conduct research and other studies related to the District curriculum. Students will be informed of their rights and responsibilities as users of the technology and communication resources prior to gaining access to them. Parents may deny access for minors (form included at the end of this policy).

There is a wide range of material available on the Internet, some of which may not fit with a particular family's values. 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. In light of these responsibilities, there is hardware and software in place to filter and block inappropriate sites and high risk activities. The District reserves the right to block sites that do not enhance classroom activities. 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 from I & T Services to blocked sites in curriculum related circumstances.

The use of an Internet filter does not diminish the user's personal responsibility to use the network in conformance with the standards in this policy.

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 the system will meet any specific requirements the user may have, or that it will be error-free, or that its operation will not be interrupted. The District will not be liable for any direct or 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 resources. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

Personally Owned Technology

The District recognizes that the network resources provided are available through public funding and, as such, every effort is made to allow public access to School District of Holmen's network resources where possible and where such access does not negatively impact the operations of the District. The following guidelines will be used by those wishing to connect personal technology to the School District of Holmen network.

1. Personally owned technology may be connected to the District network only through the District's publicly accessible wireless network. This network allows for filtered access to the Internet.
2. Any connected technology is to be used in compliance with District policies and rules. Any violation of such policies or rules may result in the exclusion of the device from school and/or discipline of the person who is found to be in violation.
3. The use of personal technology must be used in accordance with the overall Acceptable Use Plan.
4. Students must turn off and put away any personal technology when directed by a staff member.
5. 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.
6. 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.

7. The District accepts no responsibility for the loss, theft, or damage of personal property brought to school by staff or students.
8. Users may not install District software onto personal devices unless software is explicitly licensed for such use.

Social Media

The District recognizes the growth and potential usefulness of these social networking forums in disseminating educational information between employees and students and/or their parents/guardians. At the same time, the District must be mindful of the opportunity that social networking may create for inappropriate communications among students and/or their peers. All of the District's policies, rules and procedures of the District 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 Web 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 very 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, grandma, 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. Do not share your password with anyone.
8. Before publically supporting a website or article, make sure that you read it in its entirety.
9. Do your own work. Do not use other people's intellectual property without their permission. It is a violation of copyright law to copy and paste other's thoughts. When paraphrasing another's idea (s) be sure to cite your source with the URL. It is good practice to hyperlink to your sources.
10. Be aware that pictures may also be protected under copyright laws. Verify you have permission to use the image.
11. How you represent yourself online is an extension of yourself. Do not misrepresent yourself by using someone else's identity.
12. Online work should be well-written and follow writing conventions including proper grammar, capitalization, and punctuation. If you edit someone else's work, be sure it is in the spirit of improving the writing.
13. If you access inappropriate or disrespectful material that makes you feel uncomfortable, tell a staff member right away.

Staff may choose to use online/social networking resources for educational and communication with student/parents/community. District staff may allow students to create "accounts" approved by the district for district devices that are necessary for using "cloud" services, accessing resources, sharing information, turning in assignments, or communicating with teachers (for example). These accounts will be created in full compliance with COPA laws (all terms of agreements, including under age 13 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, then procedures to inform parents of the accounts will be used.

When deciding acceptable or unacceptable use, all district policies and student handbook guideline are applicable.

Unacceptable use of Information Technologies

Partnerships with parents and community shall help address Internet safety and appropriate use of Internet resources. Students and staff should have no expectation of privacy with regard to the use of the District's network or information, messages, files and other data stored on these systems. 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 being given. Nothing residing in a student's computer system or files or the District's e-mail system will be deemed personal, private or confidential.

***Cyberbullying is defined as "willful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices."**

All Students, Staff and Guests

The following activities are **NOT permitted** and will result in an investigation and potential disciplinary actions:

- Using obscene or inappropriate language or content.
- Sending or posting cruel or threatening messages or images (**also known as examples of cyberbullying**)
- Downloading, displaying, viewing, accessing or attempting to access, storing or transmitting any images, cartoons, messages or material which that may be construed as threatening, harassing, offensive or intimidating (**also known as examples of cyberbullying**) to others based upon gender, race, national origin, age, disability, religion, sexual orientation or any other basis protected by applicable law.
- 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.
- Using technology and/or communication resources for commercial or political purposes
- Use which is illegal, including the violation of copyright, defamation, gambling and pornography laws
- Damaging any component of the District's computer hardware or software
- Occupying excessive file storage space on District servers
- Unauthorized accessing or attempting to access confidential District information, including personnel records, medical records and financial information pertaining to the District or any of its employees or students
- Unauthorized accessing or attempting to access another employee's or student's password, data, messages or other electronic communication's materials (Statute 943.70)
- 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
- Re-posting a message that was sent to the user without permission of the person who sent the message
- Pretending to be someone else and sending or posting material that makes that person look bad or places that person in potential danger
- 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
- Wastefully using information technology resources such as printing
- Sharing account information with others
- Failing to protect confidential information
- 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).
- Any use that is inconsistent with the school's Code of Conduct
- Use of personal e-mail for District Business

Violations

1. Violations may result in a loss of access 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.
2. Disciplinary action may be determined at the building level in line with existing practice regarding inappropriate language or behavior.
3. When applicable, law enforcement agencies may be involved.

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.



School District of Holmen

ACCEPTABLE USE CONSENT FORM

PARENT OR GUARDIAN

I have read the School District of Holmen's Acceptable Use Policy and agree to all the terms therein.

_____ I give my permission for my child to utilize the school District's information and technology resources and certify that the information contained on this form is correct.

Signature of parent or guardian _____

Home Address _____

Home Phone Number _____ Date _____

STUDENT

I understand that my computer use is not private and that the District will monitor my activity on the computer system. Computers are tools to be used for educational purposes.

I have read the District's Acceptable Use Policy and agree to abide by the stated provisions. I understand that violation of these guidelines may result in suspension or cancellation of online privileges.

Student's signature _____ Date _____