HORTONVILLE AREA SCHOOL DISTRICT

Title: Acceptable Use Policy: Electronic Information System	**Date Adopted:** 5/22/00 **Date Revised:** 9/14/04 8/8/2011	**Policy No.** 2027

Policy Statement: The Board directs the District Administrator to provide training and procedures that encourage appropriate access to electronic information systems and networks by students, staff, and patrons while establishing reasonable controls for the lawful, efficient, and appropriate use and management of the system.

By providing electronic information systems a computer network for use by students, staff and patrons, the Board intends only to provide a means for educational activities and does not intend to create a First Amendment forum for free expression purposes. The use of the electronic information systems and the computer network in a K-12 public school system setting are subject to limited First Amendment rights as authorized by the United States Supreme Court. Electronic communication and information research skills are now fundamental to preparation of citizens and future employees during an Age of Information. The Board expects that staff will blend thoughtful use of such information throughout the curriculum and that the staff will provide guidance and instruction to students in the appropriate use of such resources.

Rationale: The Board recognizes that our electronic communications system (network) will allow unprecedented opportunities for students, staff and patrons to communicate, learn, access and publish information. The Board believes that the resources available through this network and the skills that students and staff will develop in using it are of significant value in the learning process and success in the future. These new opportunities also pose many new challenges including, but not limited to, access for all students, age-level appropriateness of material, security and cost of maintaining systems. The District will endeavor to make certain that these concerns are appropriately addressed, but cannot ensure that problems will not arise.

Scope: District-wide.

Responsibility: District Administrator; any member of the Administrative Staff; and all Technology Department personnel.

Implementation:

Procedures

Acceptable Use Guidelines

Network

1. Communications using information technology resources may be considered to be a public record; therefore, general rules and standards for appropriate professional behavior will apply. All use of technology and communication resources should be a positive representation of the district and must support the district's mission, vision, and values. The District reserves the right to prioritize use and access to the system, including using any filtering or log-in systems, and monitoring systems as deemed necessary.
2. Any use of the system must be in conformity to state and federal law, network provider policies and licenses, and district policy. School district information resources should not be used for commercial purposes, except in a purely incidental manner or except as permitted under other written policies of the school district or with the written approval of the district administrator having the authority to give such approval. Any such commercial use should be properly related to school district activities, take into account proper cost allocations for

district and other costs the district may incur by reason of the commercial use. Use of the system for charitable purposes must be approved in advance by the Superintendent or designee.

3. The system constitutes a public facility and may not be used to support or oppose political candidates, ballot measures or advocate for a political position.
4. The system shall not be used in any matter that disrupts the operation of the system by others; system components including hardware or software shall not be destroyed, modified, or abused in any way *(e.g., willfully or negligently introducing a virus or malware).*
5. Malicious use of the system to develop programs to harass other users or to gain unauthorized access to any computer or computing system and/or damage the components of a computer or computing system is prohibited.
6. Use of the District computers and network services must align with district policies and law, including, but not limited to, behavior related to discrimination, harassment, and inappropriate relationships.

   Examples of behaviors not permitted while using district information technology and communication resources include but are not limited to:

   - Harassing, insulting or attacking others – including, without limitation, cyberbullying. "Cyberbullying" is defined as any action taken by one person as to another person that has the purpose, intent or effect of tormenting, threatening, harassing, humiliating, embarrassing or otherwise targeting another person by using the District's computers and network service to access the Internet, interactive and digital technologies or mobile phones for such purpose. Cyberbullying involves the use of information and communication technologies to support deliberate, repeated, and hostile behavior by an individual or group that is intended to harm others.
   - Comments or images that may be discriminatory, offensive to others, threatening, hateful, harassing, insulting or defamatory.
   - Sexting. "Sexting" is defined as a slang term for the use of a cell phone or any other electronic device or computer to distribute pictures or video of sexually explicit images that are sent or received by the use of the District's computers and network service. It also includes in the definition for the purpose of this Policy the act of sending any person text messages of a sexually-charged nature.
   - Text roulette or SMS roulette by the use of the District's computers. "Text roulette and SMS roulette" are defined as the act of the composition of an electronic text message, sexually explicit or not, that is sent in random manner from the sender's contacts or in an entirely random manner.
   - Engaging in other behaviors in violation of district policy, district handbook, or any applicable law or regulation
7. Use of the system to access, display, store or distribute offensive, obscene or pornographic material is prohibited.
8. Communications using information technology resources may be considered ~~to be a~~ public record; therefore, general rules and standards for appropriate professional behavior will apply. All use of technology and communication resources should be a positive representation of the district and must support the district's mission, vision, and values. All communication must be for District educational purposes and not for personal use.
9. Wasteful use of information technology resources is prohibited.
10. All staff of the Hortonville Area School District will use all technology (all electronic devices and all public and private networks available to them in the district) in a manner consistent with the district's instructional goals, to the encouragement of good citizenship, and in keeping with community morals. Furthermore, staff will eschew any use of

technology which may cause loss of the respect of parents/guardians, the students, and/or other members of the community. Staff shall not engage in electronic activity that disrupts or compromises the learning process or distracts from the work environment. All technological resources used by or with students will be continually monitored to ensure compliance with all local, state, and federal regulations including, but not limited to, the Child Internet Protection Act (CIPA).

Guidelines for Internet Use

1. All Internet activity is logged and monitored. This information is subject to retention and review at any time.
2. Internet access is provided as a complement to traditional classroom instruction. As such, access to websites with offensive material, adult content, games or non-educational information (movie, entertainment, non-educational music sites, free web hosting sites, etc.) are strictly prohibited without regard to whether or not the system blocks such sites.
3. Any successful or unsuccessful attempts to view adult subject matter, pornography or other inappropriate or offensive materials will result in disciplinary action.
4. Students and staff are responsible for any activity that occurs under his/her account. PASSWORDS SHALL NOT TO BE SHARED. The sharing of a PASSWORD is a violation of this policy.

Guidelines for E-mail Use

1. All messages composed, sent or received on the electronic mail system are and remain the property of Hortonville Area School District (HASD). Electronic mail is not private or confidential property of students or staff and there is no expectation of privacy.
2. HASD retains the right to review, audit, intercept, access and disclose any information created, received or sent via its e-mail system at any time without prior notice.
3. The e-mail system is intended to complement classroom instruction. It is not to be used to create or transmit any offensive or disruptive messages. Messages that are considered offensive include, but are not limited to, any messages which contain sexual implications, racial slurs or any other comment that offensively addresses someone’s age, race, gender, sexual orientation/preference, physical attributes, religious or political beliefs, national origin or disability.
4. Per Wisconsin State law, e-mail is archived for no less than seven years and is subject to laws regarding Open Records.

Guidelines for Computer Use

1. All computer activity is logged and monitored. The logs are subject to unlimited retention and review at any time.
2. Communication using information technology resources may be considered a public record; therefore, general rules and standards for appropriate professional behavior will apply. All use of technology and communication resources should be a positive representation of the district and must support the district’s mission, vision, and values.
3. Users are expected to take appropriate measures to protect confidential information.
4. Never allow anyone access to a computer using your account information.
5. Never give out your password to anyone. Do not write it down. The Technology Department will never ask for your password.

Security

1. System accounts are to be used only by the authorized owner of the account for the authorized purpose. Users may not share their account number or password with another

person or leave an open file or session unattended or unsupervised. Account owners are ultimately responsible for all activity under their account.

2. Users shall not seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent other users on the system, or attempt to gain unauthorized access to the system. Trespassing in other user folders, documents, or files is not permitted.
3. Communications may not be encrypted so as to avoid security review.
4. Users should change passwords regularly and avoid easily guessed passwords.

Personal Security

1. Personal information such as addresses and telephone numbers should remain confidential when communicating on the system. Students should never reveal such information without permission from their teacher or other adult.
2. Students should never make appointments to meet people in person that they have contacted on the system without District and parent permissions.
3. Students should notify their teacher or other adult whenever they come across information or messages that are dangerous, inappropriate, or make them feel uncomfortable.

Privacy Rights

1. Expectation of privacy as to his or her Internet usage, or the privacy of any electronic mail message, file, download, note, or other data stored on or transmitted or received through any District equipment. Internet and email communications made on the computer network are considered public and are subject to open records requests.
2. The District reserves the right to inspect or monitor, access, remove and disclose any message or document created, archived, stored, received, deleted, looked at or sent with the District's computer network, including the monitoring of Internet connect times and sites accessed, at all times and without notice. Users suspected of inappropriate or prohibited computer network use shall be investigated.
3. To the extent practical, steps will be taken to ensure the security of users and network resources. No computer security system, no matter how elaborate, can prevent unauthorized people from accessing stored information. Therefore, users are advised that the district cannot guarantee confidentiality or that the computer network will be secure at all times.

Copyright

1. As aligned with the Board's copyright policy, unauthorized posting and copying of protected material is prohibited. Copyrighted material may not be posted on the District's Internet site or disseminated as an attached copy to an email message without authorization from the publisher with exception of the use of copyrighted material consistent with the "fair use doctrine." The unauthorized installation of software on the District's computer system is prohibited by the District.

Technology Purchases

1. All computer-related hardware and software intended for installation on the District's system or any District equipment must be approved by the Hortonville Area School District Information Technology Department before purchase.
2. Send related materials (website, information packet, demonstration copy, etc.) to the Technology Office located in the Hortonville High School or via help@hasd.org .

General Use

1. Diligent effort must be made to conserve system resources. For example, users should frequently delete E-Mail and unused files.

2. No person shall have access to the system without having received appropriate training; a signed Individual User Release Form must be on file with the District. Students under the age of 18 must have the approval of a parent or guardian.

3. Nothing in these regulations is intended to preclude the supervised use of the system while under the direction of a teacher or other approved user acting in conformity with district policy and procedure.

Monitoring, Supervision, Enforcement, and Penalties

1. From time to time, the District will make a determination as to whether specific uses of the system are consistent with the regulations stated above. Under prescribed circumstances non-student or staff use may be permitted, provided such individuals demonstrate that their use furthers the purpose and goals of the District.
2. For security and administrative purposes, the District reserves the right for authorized personnel to review system uses and file content. The District reserves the right to remove a user account on the system to prevent further unauthorized activity. The District reserves the right to deny access to any person for any reason.
3. STAFF sanctions: Violations of the conduct proscribed in this Acceptable Use Policy may result in a loss of the staff member's access to district network resources and/or other disciplinary action. The level of discipline will be determined by a consideration of the staff member's prior disciplinary record, the severity of the violation, the harm caused and other relevant factors. When applicable, law enforcement agencies may be involved. Discipline may range from a written reprimand up to and including termination of employment.
4. STUDENT sanctions: Violations may result in a loss of access and/or other disciplinary action, including suspension and expulsion. The level of discipline will vary based on the student's disciplinary record, the severity of the violation, the harm caused and other relevant factors. Disciplinary action may be determined at the building level in line with existing practice regarding inappropriate language or behavior. 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 electronic computer services may appeal in writing to the building principal.

Cross References:	Policy #2014 Public Records Policy Policy #2028 Copyright Policy Policy #4016 Sexual Harassment Policy #5003 Disciplinary Actions Policy #5007 Student Records Policy #5032 Student Handbook Policy Policy #5037 Student Use of Electronic Equipment Policy #5052 Student Conduct Policy #5054 Pupil Harassment Policy #5062 Student Use of the Internet Staff Handbook
Legal References	Section 118.125 Wis. Stats. Student Records Section 120.13(1) Wis. Stats. Student Conduct Rules/Discipline Section 943.70 Wis. Stats. Computer Crimes Section 947.0125 Wis. Stats. Computer Harassment PL 94-553 Federal Copyright Law Children's Internet Protection Act (CIPA) Children's Online Privacy Protection Act (COPPA) Family Education Rights and Privacy Act (FERPA)

Hazelwood School District et al. v. Kuhlmeier et al., 484 U.S. 260 (1988)
Morse v. Frederick, 551 U.S. 393 (2007)