ACCESS TO TECHNOLOGY RESOURCES

Purpose

The District provides access to electronic networks, including access to the Internet, as a part of the instructional program. The use of the District's property must be for educational and research purposes consistent with the educational objectives of the District. The District reserves the right to monitor and access all use and content on the District's computers and networks. No person or user should have an expectation of personal privacy in connection with their use of District's computer or networks or content stored in, created, received or transmitted over any District property unless such right is guaranteed by statute or other law.

In order to protect the integrity of the District's property and to protect the interests of the District and its students, the District prohibits (1) use that causes congestion or disruption to the computers and network; (2) searching, retrieving, transmitting or viewing any content in emails or other communications or documents that are not intended for that person; (3) unauthorized software use or downloading or installing unauthorized software, programs or files; (4) use of the network for non-District business including commercial activities, product advertisement, financial gain or political activity; (5) engaging in any illegal or inappropriate conduct, including but not limited to copyright infringement, plagiarism, piracy, harassment, bullying and cyberbullying, intimidation, threats, defamatory conduct, or misrepresentation including the unauthorized use of passwords or identities of other persons; (6) using District computers or network to photograph or videotape a student, staff member or volunteer without their consent.

Students are responsible for exercising good behavior when using District computers and networks, and users are responsible for complying with all policies. Students are expected to take responsibility for conducting themselves in an appropriate, efficient, ethical, and legal manner when using the District hardware, software, network resources, and accessing the Internet. The use of information technology resources is a privilege, not a right. Any student's failure to exercise good behavior, to comply fully with this policy or to fail to fully comply with other policies shall warrant serious consequences including, but not limited to, loss of computer and network privileges, detention, suspension, expulsion, and/or legal action. Users are notified that sexually explicit or pornographic content has no place in the District and violators who use or access such content, or photograph or videotape students/staff/volunteers in a state of undress will face severe consequences, which may include expulsion and/or legal action.

A. **School District Technology Devices**

The use of technology that is owned or leased by the District is subject to terms of this policy. Technology is defined as including, but not limited to the use of audio, video, and computer software, computers, peripherals, network and communications equipment and related hardware and video equipment. District technology is to be used to enhance instruction, support learning and/or to develop professionally.

B. **Personal Technology Devices**

The conditions set forth in this policy also apply to the use of student or employee owned laptops, netbooks, tablets, smart phones, e-readers, music players, digital cameras, flash drives, and any and all other personal computer or storage devices. Personal technology, when used in the school is bound by the same guidelines as District owned equipment and is to be used to enhance instruction, support learning and/or to develop professionally.

Description of Security Measures

The Internet provides access to a wide range of material. The District expects that staff shall blend thoughtful use of the Internet throughout the curriculum. Because technology is constantly evolving, it is impossible for school personnel to review and pre-select all materials that are appropriate for the use of students and employees.

1. **Filtering** – To the extent practical and consistent with legal requirements, the District shall use commercially reasonable technology protection measures (or "Internet filters") that allow it to meet the requirements of the Children's Internet Protection Act, including the use of a filter to protect against access to:
   a. Material that is, by definition, obscene (section 1460 of title 18, U. S. Code)
   b. Child pornography (section 2256 of title 18, U.S. Code)
   c. Material that is harmful to minors (further defined in the Children's Internet Protection Act)
      1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
      2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and SEXUAL ACT; SEXUAL CONTACT. The terms "sexual act" and "sexual contact" have the meanings given such terms in section 2246 of title 18, United States Code.
      3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

2. **Supervision** – Since no technology protection measure will block one hundred percent of the inappropriate material, the District emphasizes the importance of supervision. It is the expectation that all District staff shall be responsible for monitoring and supervising all users of information technology resources, including the Internet.

3. **Education** – Education about online behavior, including interacting on social networking sites and chat rooms, as well as issues surrounding cyberbullying awareness and response, and protecting children from cybercrimes, including crimes by online predators, shall be covered in the curriculum each school year.

Administration, Monitoring, and Privacy Rights

The District owns its computers, its networks and the content on those computers and networks. The District may enforce the operation of technology protection measures at any time and during any person's use of the District's network. To insure system integrity and appropriate use of information technology resources, the District reserves the right to monitor, inspect, store, and copy any information transmitted, stored, or received using information technology resources. Users shall have no expectation of privacy regarding the use and content in information technology resources. In certain limited circumstances reserved to the discretion and decision of the District Administrator or designee, the technology protection measures may be disabled, circumvented, or minimized for those demonstrating a bona fide research need to access such filtered or blocked materials, or for other lawful purpose.

Statement Prohibiting Use Related to Discrimination, Harassment, and Defamation

The District prohibits use of its computer system for any purpose in violation of the District's discrimination and anti-harassment policies. All forms of harassment through the use of technology commonly referred to as cyberbullying, are unacceptable and viewed as a violation of this policy. Cyberbullying includes, but is not limited to the following misuses of technology: harassing, teasing, intimidating, threatening, or terrorizing another person by sending or posting inappropriate and hurtful email messages, instant messages, text messages, digital pictures or images, or website postings. The District's computer system may not be used to defame others or disclose sensitive personal information about others.

Copyright Infringement of Software

The District prohibits the unauthorized use, downloading, installation, or copying of software on the computer system. All software used, downloaded, installed or copied must be approved by the District. All users must comply with applicable licensing agreements and copyright laws, and copyrighted material may not be used or shared without authorization from the publisher.

Use of Personal Technology & Devices

Personal technology devices may be used in the school buildings as determined by the building principal and technology director, or designee. Under no circumstances are personal technology devices to be used during a test or assessment unless permission is granted by the classroom teacher.

Printers, wireless devices, switches, routers, hubs, servers, hotspots or any other device that may extend network services may not be connected to the District network except as otherwise authorized.

1. Students shall follow all provisions of the District acceptable use policy and agreement.
2. The District reserves the right to deny the use of personal technology devices based on adherence to policies and procedures, and may take disciplinary action for inappropriate use.
3. The student assumes all liability for damage, theft, or loss of personal devices.
4. The student is responsible for locating secure storage for his/her personal device as needed during the school day.
5. Students understand that accessing the District network with their personal device will be limited to the internet via a guest wireless connection.
6. Personal devices brought to school must have up-to-date anti-virus software to protect against virus transfers. Owners of personal technology device may not use the device to propagate a virus, worm, Trojan horse, spyware, or other malicious software on the District network.
7. Students may not use personal technology devices during instructional time unless approved by the building principal.
8. Students may not use personal technology devices during a test or assessment unless permission is granted by the classroom teacher.
9. Students may not use personal technology devices to disrupt the school climate.
10. Students may not use personal technology devices to obtain unfiltered internet access while on District property.
11. Students may not use personal technology devices to take photographs or record audio or video while on District property or while engaged in a school-sponsored activity unless approved by the building principal or classroom teacher, in accordance with District policies.

12. Students may not use personal technology devices to establish a wireless network or "hotspot."
13. Students may not use personal technology devices to access, create or send inappropriate content while on District property or at school-sponsored events.
14. The operation and connectivity of a personal device is the responsibility of the individual. The District does not provide technology support for personally owned devices.
15. The District makes no warranties; neither expressed nor implied that the services provided by the District system shall be error free. The District shall not be responsible for any damages users suffer, included but not limited to, lost data or interruptions of services.
16. The student is responsible for sufficiently charging battery resources for devices (power outlets may or may not be available or within reach in the classroom).

Description of Other Unacceptable Uses

District resources are to be used for school-related administrative and educational purposes. The user is responsible for his or her actions and activities involving technology. Before using the District's network/Internet, students and their parents/guardians must first read and sign the Access to Technology Resources Consent Form, and have it on file in the school's library media center (LMC).

Some examples of prohibited uses include, but are not limited to, the following:

- Searching for or deliberately viewing, listening to or visiting websites with or known for containing inappropriate material or any material that is not in support of educational objectives, such as profane material, obscene material, sexually explicit material or pornography.
- Attempting to vandalize, change computer settings, damage, disconnect or disassemble any network or computer component.
- Attempting to gain unauthorized access to the District system or to any other computer system through the District system, or beyond an individual's authorized access. This includes attempting to log in through another person's account or accessing another person's files with or without their permission.
- Searching for or creating security problems as this may be construed as an unauthorized attempt to gain access, i.e., computer hacking.
- Using District resources for purposes of plagiarism, theft, infringement and other illegal or illicit purposes.
- Installing or downloading software without permission of the Director of Technology or his/her Designee or using District software in a manner inconsistent with the District's interests, license agreements and applicable laws.
- Wasting District resources including bandwidth.
- Bypassing or attempting to circumvent network security, virus protection, network filtering, or policies.
- Revealing personal data of students and staff (example: PIN, social security number, credit card numbers, addresses, phone numbers, etc.),
- Using the system for purposes unrelated to the interests of the District such as use for commercial purposes or personal pleasure or gain.
- Taking photographs, recording audio or video while on District property or a school-sponsored activity unless approved by the building principal or classroom teacher, in accordance with District policies

Use of Social Networking Sites

Online communication is critical to our students' learning of 21st Century Skills and tools. Blogging and podcasting offer an authentic, real-world vehicle for student expression. Certain Web 2.0 services, such as Moodle, wikis, podcasts, RSS feeds and blogs that emphasize online educational collaboration and sharing among users, may be permitted by the District. However, such use must be approved by the Director of Technology or designee, followed by training authorized by the District. Users must comply with this policy as well as any other relevant policies and rules during such use.

Monitoring, Supervision, Enforcement, and Penalties

Consequences for violations of the Acceptable Use Policy include, but are not limited to, the following:

- Employee discipline
- Suspension or revocation of Internet/Network privileges
- Student detention, suspension or expulsion
- Restitution for the cost of the repair and/or technician fees to repair
- Legal action and prosecution by the authorities

LEGAL REF: 118.001 Wisconsin Statutes
120.44
943.70(2)
947.0125
Children's Internet Protection Act
Neighborhood Children's Internet Protection Act
Children's online Privacy Act
Federal Copyright Law [17 U.S.C.]
Technology Education and Copyright Harmonization Act (TEACH Act)
Broadband Data Improvement Act of 2008 (Title II – Protecting Children in the 21st Century Act)

CROSS REF: 363.2-Exhibit (1), User Agreement and Parent Permission Form (PK-12)
110, School District Mission and Goals
330, Curriculum Development and Improvement
347-Rule, Guidelines for the Maintenance and Confidentiality of Student Records
361.1, Selection of Textbooks and Related Materials
363.3, Technology Concerns for Students with Special Needs
411, Equal Educational Opportunities
411.1, Harassment
443, Student Conduct
443.5, Student Possession and Use of Two-Way Communication Devices
443.7, Academic Integrity
443.71, Bullying Prevention
447, Student Discipline
512, Staff Non-Discrimination
522.7, Employee Use of Electronic Communications
561, Staff Internet Access/Web Page Consent Form
771.1, Copyright Policy

823, Access to Public Records
871, Public Complaints Textbooks and Other Instructional Materials
Student Handbook

APPROVED: September 21, 1998
July 14, 2003
July 18, 2011
January 21, 2013
December 21, 2015
APRIL 22, 2019