COMPUTER, INTERNAL NETWORK, ELECTRONIC MAIL, AND INTERNET ACCEPTABLE USE POLICY FOR STUDENTS

The School District of West Allis West Milwaukee, et al., uses technology resources to support and enhance established curricular goals and academic success as outlined by the Department of Instructional Services.

- "Technology resources" are defined as laptop and desktop computers, cell phones, smart phones, telephones, tablets, servers, e-readers, storage media, handheld devices, printers, scanners, software, facsimile machines, and any other District-owned or contracted-for electronic communication equipment.
- Technology resources are classified as school property, and are owned by the District and are subject to the District's rights under contract and law. Technology resources must be used efficiently in the interests of the District and for the educational purposes for which they were intended. Users are required to follow the guidelines outlined in this Policy, as well as other school rules and related policies.
- "Web resources" are a collection of tools that enable interaction on the Internet and include, but not limited to, blogs, wikis, podcasts, social media, email, and other forms of electronic communication. The District provides access to many hosted (in-District) web resources for use by its staff and students.

Limitations

Technology resources provided by the District are for educational purposes only. Acceptable uses are those which support the District mission, vision, and Strategic Plan. Technology resources, like any other school property, are owned by and the property of the District and subject to the District's rights under contract and law. At any time without warning, the District may remove computer software and move or delete data stored on networked systems.

The use of technology resources and web resources are considered an extension of the classroom.

- Compliance with all District policies, guidelines, rules, and acceptable standards of behavior are necessary and required.
- The District emphasizes to all users that access to technology is a privilege not a right; therefore a user will be held responsible for his/her actions while using the technology system.
- Inappropriate use of electronic information resources can be a violation of local, state, and federal laws and can lead to prosecution under those laws.
- Students failing to abide by the Appropriate Use Policy may lose network/computer privileges along with consequences that may arise from violations of normal school rules and District Handbook guidelines, up to and including possible expulsion.

Property of the District, No Expectation of Privacy

Users should have no expectation of privacy in the contents of any communications or files on District technology resources, individual storage systems, or Web resources unless such expectation is granted by law. The District maintains the right to access, inspect, investigate, and monitor all use and its technology resources, including all files, communications and information created on, with or transmitted using its technology resources or Web resources, and including e-mail, text messages, internet usage, and any other communications or information, without notice to or consent of the user. All such files, communications, or information can be reviewed by the District for any purpose and at any time, and may be subject to monitoring, review and disclosure pursuant to civil and criminal matters, investigatory purposes, or any other lawful reason.

Responsibilities and No Liability of the District

The District technology system shall be used in a responsible, efficient, ethical, and legal manner, and all users shall abide by the District's policies and procedures. It is essential that each student recognize his or her responsibility in having access to services, sites, and people that the network provides. The user (student) is ultimately responsible for his or her actions. Parents and guardians must set and convey high standards that their children should follow when using technology resources.

- The District uses a filtering system in an attempt to limit student access to material that is harmful to students, obscene or disruptive to the educational or work environment.
- The District reserves the right to block sites that do not enhance established curricular goals. The District shall be in compliance with the Children's Internet Protection Act (CIPA).
    - Although CIPA defines "minor" as any individual who is under the age of 17 years, district policies will apply to all students, regardless of age.
- No technology measure can block 100% of inappropriate content so the District emphasizes the importance of staff supervision in monitoring student use of technology.
    - Access to the Internet provides connections to other computer networks and personnel all over the world, users should understand that the District does not control the content of information available on such networks.
    - The District is not responsible for the accuracy, quality, or appropriateness of the information obtained through the Internet and makes no warranties of any kind, either expressed or implied, that the information or services contracted by or through the Internet will be error-free or without defect.
    - The District is not liable for any damage suffered by a user of the system, including but not limited to, loss of data stored on or transmitted by technology resources or interruptions of service.
    - The District is not responsible for any mistakes or negligence, liability, copyright infringements or other costs incurred by the person using the District's technology resources.

If a user inadvertently becomes connected to a site that contains material with prohibited content, the user must disconnect from that site immediately and inform a staff member of the incident. Students are encouraged to inform a staff member if they are aware that another user is accessing or has accessed prohibited material via the District's technology resources.

Education, Supervision, and Monitoring

It shall be the responsibility of all instructional members of the District staff to educate, supervise, and monitor appropriate use of the technology resources, including access to the Internet in accordance with this policy.

The District will promote safe online activity for students and educate students about appropriate online behavior, including interacting with other individuals on social networking websites and cyberbullying awareness and response. This includes, but is not limited to:

- Teaching students how to locate and evaluate appropriate electronic sources;
- Teaching students information literacy skills, including understanding of safety, copyright, ethical practice and data privacy; and,
- Teaching students proper safety procedures when using e-mail, social networking websites, texts, and other forms of direct electronic communication.

Use and Guidelines of the District Technology System

1. All use of District technology resources, including access to the Internet, must be in support of the educational goals of the District. All Board, student Handbook, and school policies must be followed when using any technology resource.

2. Use of District technology to access and/or distribute any material that violates U.S., state, or School Board policy is prohibited.

3. Use of technology to access/use copyrighted materials, pornography, materials harmful to minors, obscene materials and/or similar materials is prohibited.

4. Students may not use the District's technology system in an offensive, harassing, illegal, or defamatory manner. Hate mail, harassment, discriminatory remarks, cyber bullying, and other antisocial behaviors are unacceptable in Internet and other network communications. The District prohibits the use of the system to send or receive offensive or improper messages such as derogatory messages about other students or staff members. In addition, the District prohibits the use of the technology system in any way that could be construed as harassment or disparagement of others.

5. Use of proxy sites to bypass District web filters is prohibited.

6. All information accessible through the Internet should be assumed to be private property and subject to copyright protection. Internet sources should be credited appropriately, as with the use of any copyrighted material.

7. Students have a responsibility to respect the privacy and property of other users. Students should not intentionally seek information about, obtain copies of, or modify, files, data or passwords of other users. A student will not allow another student to access computers or network resources using his/her login credentials.

8. For their own safety, students should not reveal any personal information, such as last names, addresses, phone numbers, or photographs.

9. Employing the Internet for commercial purposes is prohibited. Students may not use the system to solicit for commercial activities, religious or political causes, outside organizations or other non-school related matters without prior authorization from the building principal.

10. Students should not expect that files stored on district servers will always be private. School and network administrators may review files and communications to maintain system integrity and to ensure that the network is being used responsibly.

11. Technology resources must be handled with care. Physical damage or network interruptions such as the introduction of viruses or deleting of files are prohibited.

12. No eating or drinking near computers.

13. Students are directed to keep passwords for their own private use and should log-off network when leaving the desktop station.

14. Students may not access social networking sites (such as MySpace, Facebook, Instagram, SnapChat,etc.), personal websites, personal blogs, online gambling sites or personal email accounts on District computers except for educational purposes specifically approved by the classroom teacher. Students may not engage in cyber-bullying activities.

15. Students may not load, save, download, or otherwise install software on technology without approval from the District technology department.

16. Students who create web pages, blogs, profiles or other online postings outside of school that result in the student's online posting being accessed and viewed in the school environment may be disciplined if there is a disruption at the school as a result of the online posting.

17. Students may not use the District's technology system to develop programs or to institute practices that harass other users or gain unauthorized access to any entity on the system. Students may not damage the components of an entity on the system.

18. Students should not share documents, emails, blog postings or any other information created by someone else unless specifically permitted to do so by the creator.

Student Owned Technology – Outside of School

Students' home and personal Internet or other communication tool technology use can have an impact on the District, school and on other students. If a student's personal Internet expression, such as a threatening message toward a staff member or another student, or a website advocating violence or defamation of another's character, creates a substantial disruption at school, offenders may be subject to school disciplinary action and/or legal action.

Substantial disruption is defined as any of the following:

- Necessary cessation of instruction or educational activities;
- Inability of students or educational staff to focus on learning or function as an educational unit because of a hostile environment (including cyberbullying);
- Severe or repetitive disciplinary measures are needed in the classroom or during educational activities;
- Exhibition of other behavior by students that substantially interfere with the learning environment; or,
- Other similar disruption.

Student Owned Technology – Inside School

Students may bring technology into the District, including laptops, smartphones, mp3 players, etc. The District is not responsible for the security or safety of student owned technology while on school property or under supervision of a school authority.

- Students must follow the school rule regarding use of that technology during the school day. This typically will include not using the technology during class time, as the District has provided technology to students where appropriate for reaching established educational goals.
- Students who use student-owned technology while on District property, outside of the school day, must follow all rules and guidelines of this Acceptable Use Policy.
- Administrators may confiscate and search student-owned technology while on District property if the administrator has reasonable suspicion that the use of the technology is in violation of this Acceptable Use Policy, school rules, or state law.
- Student owned technology may be confiscated, but not searched, by classroom teachers for the length of the class if the student or technology is creating a disruption.
- During emergencies, the District may require student owned technology to be turned off so emergency networks are not overwhelmed.

Consequences

Inappropriate use of the District's technology resources, Web resources or District property and any other violation of District policies, guidelines or rules may result in suspension of technology privileges, report to criminal authorities, legal action, and discipline up to and including suspension and expulsion for students, in accordance with the Student Handbook. Appeals may be made in accordance with appropriate Board Policies and procedures.

Failure to follow the Acceptable Use Guidelines may result in disciplinary actions including loss of technology privileges, suspensions, expulsions or, when applicable, law enforcement involvement.

- Individual school sites have the liberty to create a system of classroom and school-wide rules, consequences, and policies in accordance with the "Student Owned Technology-Inside School" at the individual school level that is relevant to their school and student body. These will be developed with school staff and will be communicated to students as part of schoolwide behavior expectations.
- If a student fails to comply with the school rules, the student will receive consequences that are outlined by the school policy.
- At any time, the district can and will review the individual procedures being utilized in each school and make changes as necessary.

Parental Opt-Out Provision

The District will provide students access to technology resources, including the Internet, unless the parent/guardian notifies the appropriate building principal in writing that the District should prevent access to technology resources for his/her student(s). Parents or guardians have the right to view contents of their child's user account or network activity, if possible, accessible, and within the confines of applicable law, or to revoke their child's technology permissions, upon written request.

Investigations

The District will cooperate fully with local, state and federal officials in any investigation concerning or relating to any illegal activities conducted through the District's system. In the event that there is an allegation that a student has violated the District's policy, an investigation will ensue with the possible end result being that technology privileges may be withdrawn from students who do not respect the rights of others and who do not abide by established District policy or other discipline up to and including possible expulsion. Specific disciplinary actions will be tailored under guidance of the School District Rights and Responsibilities Handbook to meet the specific concerns related to the violation, as well as local, state and federal law.

LEGAL REF.: Sections 120.13 Wisconsin Statutes
943.70
947.0125
968.27 – 968.27
Electronic Communications Privacy Act of 1986

CROSS REF.: 363.2-Rule, Computer, Internal Network, Electronic Mail, and Internet Acceptable Use Policy for Students

APPROVED: May 5, 1995

REVISED: June 11, 1996
February 24, 2003
June 14, 2010
April 9, 2012
August 14, 2017