POLICY 363.2

INTERNET SAFETY AND ACCEPTABLE USE

Consistent with applicable federal laws, the Platteville School District Board believes that the best approach to student safety as it relates to use of the Internet and other electronic resources involves a combination of technology protection measures, monitoring and instruction. The District's comprehensive approach to student Internet/technology safety shall take into account the differing ages and instructional levels of the students in the District.

It shall be the responsibility of the Director of Technology to:

1. Ensure that the District's systems and equipment that provide access to the Internet make active use of technology protection measures designed to block or filter Internet access to visual depictions that are:

   a. obscene;
   b. pornographic; or
   c. as to computers and other devices that may be accessed by students or other minors, otherwise harmful to minors.

   Filtering, blocking or other protective technologies will also be used to decrease the likelihood that student users of the District systems and equipment might access other materials or communications, other than visual depictions, that are inappropriate for students. Recognizing that there will always be room for possible improvement in connection with the District's efforts at prevention, all employees, parents and guardians, and students are encouraged to report to the Director of Technology or Building Principal, any complaints or concerns regarding student access or exposure to any content, activities or communications that may be harmful, deceptive, or otherwise inappropriate or objectionable.

2. Develop and implement procedures that provide for the monitoring of students' and other authorized users' activities when using District-provided equipment or District-provided network access or Internet access. Such monitoring may sometimes take the form of direct supervision of students' and minors' online activity by school personnel, but the Board recognizes that constant, direct supervision is not a practical expectation.

3. Develop and implement an instructional program that is designed to educate students about acceptable and responsible use of technology and safe and appropriate online behavior, including (a) safety and security issues that arise in connection with various forms of electronic communication (such as e-mail, instant messaging, and similar technologies); (b) interacting with other individuals on social networking sites and in chat rooms; and (c) cyberbullying awareness and response. Such educational activities shall include (but shall not consist exclusively of) reinforcement of the provisions of the District's rules regarding students' acceptable and responsible use of technology while at school.

4. Maintain, revise and enforce rules and procedures concerning the acceptable, safe, and responsible use of the District's Internet access infrastructure and other technology-related

District resources by any person who is authorized to use the District's systems and equipment, including any student, District employee, District official, or other authorized user. These rules and procedures shall complement structural and systemic supports that are implemented to further encourage and facilitate the acceptable, safe, and responsible use of the District's technology-related resources. To the extent appropriate to various groups of users, and with all such additions as the administration deems necessary or appropriate, those rules and procedures shall:

a. Address and prohibit the unauthorized collection, disclosure, use and dissemination of personal and personally-identifiable information regarding students and minors, as particularly applicable to technology-based resources;
b. Address employees' obligations regarding the proper retention of District records, maintaining the confidentiality of student records, and avoiding inappropriate disclosures of District records;
c. Prohibit unauthorized user access to systems, networks and data;
d. Prohibit the use of District resources to access and/or transmit inappropriate material via the Internet, electronic mail, or other forms of electronic communications;
e. Provide notice to users that there is no District-created expectation of privacy in their use of District technology resources. Accordingly, except where prohibited by state or federal law: (1) the District reserves the ability to track, monitor, and access all data, files, communications, or other material that users create, store, send, delete, receive, or display on or over the District's Internet connection, network resources, file servers, computers or other equipment; and (2) all aspects of any individual's use of the District's technology-related equipment and resources, including any online activities that make use of District-provided Internet access, may be monitored and tracked by District officials; and
f. Provide notice to users regarding possible consequences for violations of the policies, rules and procedures that govern the acceptable, safe, and responsible use of the District's technology-related resources.

Building Principals shall have responsibility, within their respective schools, for overseeing the day-to-day implementation of the District's policies, rules and guidelines regarding the acceptable, safe, and responsible use of technology resources. A Building Principal, in consultation with the District's Director of Technology, as needed, may approve modified levels of Internet filtering/blocking for an individual user account provided that there is a legitimate educational purpose and any changes in access will not compromise the overall adequacy of protections that are in place for student users.

Legal References:

Wisconsin Statutes

Section 120.12(1) [school board duty; care, control and management of school property and affairs of district]
Section 120.13(1) [school board power to adopt conduct rules and discipline students]
Section 120.18(1)(i) [report on technology used in the district]

Section 943.70 [computer crimes]
Section 947.0125 [unlawful use of computerized communication systems]
Section 995.55 [access to personal Internet accounts]

Wisconsin Administrative Code

PI 8.01(2)(k) [integration of technology literacy and skills in curriculum]

Federal Laws and Regulations

Children's Internet Protection Act (CIPA) and Neighborhood Children's Internet Protection Act (NCIPA) [policy and other requirements related to Internet safety]
Protecting Children in the 21st Century Act [Internet safety policy requirement; education of students regarding appropriate online behavior]
Children's Online Privacy Protection Act (COPPA) [parent control over personal information collected by websites from their children]
E-rate funding requirements [technology plan and other requirements]

Cross References:

Adoption Date:

First Reading: July 9, 2018
Second Reading: August 13, 2018

School District of Platteville
Platteville, Wisconsin

POLICY 363.2 RULE

STUDENT ACCEPTABLE USE OF TECHNOLOGY RULES

A. Overview of Acceptable Use

The District's technology resources, including the District's technology-related equipment, software, networks, network connections, and Internet access, are open to limited and regulated use by students as a privilege. Each student who uses the District's technology resources is required to follow the District's established expectations for acceptable use.

In general, "acceptable use" means that a student is required to use technology resources in a manner that:

1. has a legitimate educational or other school-authorized purpose;
2. is legal;
3. is ethical (including, for example, avoiding plagiarism);
4. avoids harm to any person (including, for example, making threats, harassing or bullying someone, violating someone's privacy, accessing another person's accounts, records or files, etc.);
5. avoids harm to property (including, for example, damaging hardware, software, equipment, another person's work or electronic files, etc.);
6. avoids accessing or transmitting harmful or inappropriate material;
7. is respectful of others; and
8. is consistent with all applicable school notices, rules, and regulations, as well as any additional directives or instruction that may be provided by District staff.

Students should approach their use of technology resources with the understanding that all of the school rules and expectations that apply to in-person interactions and to the student's general conduct while at school or while under the supervision of a school authority also apply to their use of District technology, their online conduct, and their electronic communications. This document and various other District policies, rules and regulations include additional requirements and expectations that are directly related to the use of technology resources and electronic devices.

Policies, rules, and regulations cannot directly address every situation that a student may encounter. Therefore, an additional aspect of "acceptable use" is that the District expects each student who uses District technology resources to take an appropriate degree of personal responsibility for exercising sound judgment in his/her use of technology and in his/her technology-related activities and communications.

If a student has a question concerning any policy, notice, rule, regulation or directive that relates to technology resources, or if a student encounters a situation in which they are uncertain about any expectation for acceptable use or about how to proceed, the student should contact a teacher or an administrator to obtain appropriate guidance.

B. Notices and Warnings to Students Who Use School District Technology Resources

1. The District owns, controls, and oversees all of the schools' technology resources, including the District's technology-related equipment, software, applications, networks, network connections, and Internet access.

2. Unless otherwise prohibited by law, at all times and without further notice:

    a. Each user of District technology resources is subject to direct and regular District oversight of, and District access to, any and all data, files, communications, or other material that the user creates, stores, sends, deletes, receives or displays on or over the District's Internet connection, network resources, file servers, computers or other equipment.
    b. All aspects of any individual's use of the District's technology-related equipment and resources, including any online activities that make use of District-provided Internet access, are subject to monitoring and tracking by District officials.

3. Except as to any privacy rights that independently exist under state or federal law, no person who accesses and uses the District's electronic networks and other technology-related equipment and resources does so with an expectation that any privacy right exists that would prevent District officials from (a) monitoring the person's activities; or (b) accessing any user's equipment, data, communications, and other materials.

4. Any person who uses the District's technology resources does so solely at their own risk regarding possible damage to or any other potential loss of data, content, software, or equipment. This includes loss of data for any reason whatsoever, including the District's own negligence, errors, or omissions. The District offers no warranties or remedies to users regarding any damage, deletion, or other loss of user property/data. Further, except as to any mandatory duties imposed by law, the District makes no promises or warranties of any kind, whether expressed or implied, for the technology-related services it provides. The District is also not responsible for the accuracy or quality of non-District content obtained through the District's technology resources.

5. If a student wishes to use technology (including engaging in electronic communications) in a manner that is secured, private, and not accessible to the District, he/she should <u>not</u> use the District's technology resources.

6. If a student uses District technology resources in a manner that violates the District's expectations for acceptable use, or any other established policy, regulation, rule, or directive, the student is subject to possible discipline. Examples of possible consequences for improper use of technology include the following:

    a. Suspension, restriction, or revocation of the privilege of use of District technology resources;
    b. The imposition of academic consequences for academic-related violations;
    c. Suspension and/or expulsion from school; and/or
    d. Referral to law enforcement.

C. Additional Rules, Regulations, and Expectations for Student Users

1. THE STUDENT MUST BE AN AUTHORIZED USER. No student shall use District technology resources unless he/she is currently an authorized user, as determined by the District.

    a. The primary step in becoming an authorized user for any student in grade 5 or above is that the student and the student's parent or guardian must first sign a "*School Technology User Acknowledgement or Agreement*." Access to specific networks, domains, applications, etc. may be further restricted pending a determination of need and/or pending successful completion of District-specified training/instruction.
    b. The District reserves the right to deny, revoke, suspend or limit specific user accounts and/or the user's access privileges.
    c. If a student who is not an authorized user nonetheless proceeds to use District technology resources in violation of District policies and rules, all other District rules and expectations regarding acceptable use still apply to the student and may become independent grounds for discipline.

2. UNAUTHORIZED ACCESS AND OTHER PROHIBITED ACTIVITIES. Students are prohibited from engaging in (or attempting to engage in) the following conduct at all times:

    a. Installing any software programs or applications without District permission.
    b. Knowingly exposing the District's technology resources to possible viruses, malware, spyware, or any other similarly harmful material.
    c. Accessing any network, drive, file, application, database, or system that the District has not authorized for the student's use/access, including all forms of computer or computer system hacking.
    d. Modifying the security settings (including any settings or filters that limit access to particular content) on any system, network, application, portal, web site, or device.
    e. Using another person's login or password information, or allowing another person to use the student's own login or password information.
    f. Physically connecting any unauthorized personally-owned technology equipment to a District network (including computers, laptops, tablets, smart phones, printers, etc.) except for (1) authorized connections to the wireless network the District provides expressly for students and guests, if any; and (2) temporarily connecting data drives/devices to District equipment for the purpose of transferring data or files for an educational or other authorized purpose.
    g. Modifying without permission any District records, any District-controlled web pages or web-based accounts, or any of the District's Internet-based resources.
    h. Removing any unauthorized District equipment from school grounds or from its District-designated location within a building.

    i. Using District technology resources for any private commercial activities (for example, solicitations or advertisements) or for any activities that involve political advocacy connected to any election.

3. RULES AND EXPECTATIONS RELATED TO COPYRIGHT LAW, LICENSING AGREEMENTS, AND RELATED ISSUES.

a. While using the District's technology resources, students are individually responsible for following applicable laws, regulations, and agreements that relate to the use of any other person's or entity's products, services, or content.
b. Students may not use any electronic content, application, software, or technology service (1) that has not been properly purchased or licensed; or (2) in any manner that violates a license, user agreement, or the terms of use established by the owner/manufacturer/vendor of the product, service, or content.
c. Students may not use District technology resources in connection with any unlawful or any non-school related file-sharing activities, including the improper copying, storing, downloading, uploading, or transferring of copyrighted works such as music, images, video, or movies.
d. Students are expected to verify their authority (by obtaining permission when necessary) to copy, use, incorporate, or adapt any work that is subject to copyright, trademark, or other similar legal protection. This expectation applies regardless of the format of the work in question. Students are cautioned that the fact that an image, video, recording, article, file, program, book, or other work that is subject to copyright or trademark protection is available through the Internet does not mean that it is in the public domain (i.e., able to be freely used), or that it can be further used, copied, or adapted without first obtaining appropriate permission from the person or entity who holds the applicable rights.
e. Property created by a student that is submitted as an assignment or for an assessment, or for a grade or course credit, may be retained by the District as a student record and displayed for school purposes subject to laws and any District policy or procedures that govern such records. The District may further extend its right to retain, reproduce, distribute or otherwise use student-created intellectual property by obtaining specific permission from the student and the parent or guardian of a minor student.
f. To the extent consistent with applicable law, the District retains the exclusive right to determine, at its discretion, the content that is permitted to be displayed or otherwise made available to the school community and/or to the general public through the District's technology resources.

4. RULES AND EXPECTATIONS RELATED TO ACADEMIC INTEGRITY.

a. District and individual teacher expectations regarding honesty and fairness in academic contexts apply fully to activities that involve the use of technology.
b. Students may not use or access the District's technology resources in a manner that would give them an unfair academic advantage over other students.
c. Due to the scope and nature of electronic resources, the District has a heightened expectation for students who are using technology resources and/or engaging in electronic research to take special care to avoid plagiarism, which includes copying, close paraphrasing, or representing as one's own the writing, ideas, or other work of another person without appropriate attribution.

5. ELECTRONIC COMMUNICATION BY STUDENTS.

a. There are various forms of electronic communication that students may be able to access and use through the District's technology resources. Examples include course management applications that permit student submissions, email, social media

platforms, chat functionality, message boards, applications that function like text messaging, etc.

b. Students using District technology resources to engage in any form of electronic communication are expected to follow the District's rules and expectation for "acceptable use" as defined in this document, and, as far as the content and purpose of their electronic communications, students are expected to adhere to the school rules and expectations that apply to in-person interactions.

c. The following are specific examples of conduct that is prohibited in connection with a student's use of District technology resources for electronic communications:

- Electronic communications must not contain defamatory, discriminatory, threatening, offensive, racist, deceptive, sexually-explicit, or obscene content.
- Electronic communications must not be used to bully, harass, degrade, or intimidate another person.
- Electronic communications must not be used to facilitate any unlawful activity or any violation of school rules.
- Students shall not engage in electronic communications with persons who are not affiliated with the District unless the communication is for a legitimate educational or other authorized purpose and the student is reasonably sure of the identity of the person or entity with whom they are communicating.
- Students shall not attempt to access or send electronic communications using another person's account or user ID. Similarly, students shall not impersonate another person using electronic communications.
- Students shall not create, transmit, or forward messages, Internet-links, images, files, or attachments that do not have a legitimate educational purpose (for example: spam, jokes, etc.) and/or that may be harmful (for example: executable files, viruses, requests for personal or confidential information, material from an unknown source, etc.).
- Electronic communication received from another person should not be forwarded or shared gratuitously when the original sender has clearly indicated their intent that the message should not be forwarded or shared. This limitation is not intended to prevent a student from addressing a safety concern or reporting a violation of school rules by contacting a responsible adult.

d. Examples of acceptable electronic communications involving the use of District technology resources include:

- Communicating with a teacher regarding schedules, assignments, curriculum content, class projects, and class activities.
- Communicating with other students to facilitate collaboration, planning, and research for school-related projects and activities.
- When authorized by a teacher, communicating with third parties outside of the District as a means of collaborative learning, academic research, or other school-related purpose.
- Giving careful and respectful consideration to the possible consequences for others before sending, transmitting, or forwarding any electronic communications.

6. STUDENT EMAIL ACCOUNTS.

a. To promote effective communications, students will be provided District email accounts. District-provided student email accounts remain under the ownership and control of the District and student use of his/her account is a privilege.
b. Student email accounts that have been issued by the District are to be used for school-related, educational purposes only. Students are not permitted to use their school-issued email account to send or receive personal messages. If a student receives a personal email, he/she should notify the sender that such messages are not permitted.
c. A student email account provided by the District is not confidential or private, and a student's email may be read by District employees or authorized agents of the District. Students who use a District provided email account should view the messages that they send in the same manner that they view (1) verbal exchanges that occur in a classroom; and (2) assignments that are presented to a teacher. The content of emails can lead to disciplinary and other consequences.

7. STUDENTS HAVE LIMITED PERMISSION TO POSSESS AND USE PERSONAL ELECTRONIC DEVICES AT SCHOOL ("BRING YOUR OWN DEVICE" (BYOD) RESTRICTIONS)

a. A student may bring a personal electronic device to school and use the device only to the extent consistent with this document, related Board policies 443.5: Student Use of Electronic Communication Devices, and 731.1: Privacy in Locker Rooms, and any other rules or directives issued by the District or school staff to govern the time, place, and manner in which students may possess and use personal electronic devices.
b. The District assumes no responsibility for the loss or theft of, or for any damage to, any personal electronic device that a student chooses to bring to school or to a school activity regardless of (1) when the loss, theft, or damage occurs; or (2) where the device is located/possessed at the time the loss, theft, or damage occurs. The District is permitted, but not obligated, to investigate or otherwise resolve the loss or theft of, or any damage to, any personal electronic device.
c. Where the District has reason to suspect that any personal electronic device is present or has been used in violation of any Board policy or school rule, school personnel may temporarily confiscate the device. Staff shall make an effort to store a confiscated device in a reasonably secure location. To the extent consistent with applicable law, a confiscated device may be subject to a search by a school administrator or law enforcement officials.
d. Students are required to relinquish electronic devices to school personnel when directed. Refusal to comply or interfering with such a directive (e.g., by removing the battery or memory card without permission) will be considered insubordination and the student will be subject to disciplinary action.
e. Taking pictures or making or transmitting any video or audio recording of other students or school staff is prohibited at all times unless the student has obtained advance permission per District guidelines.
f. Students are strictly prohibited from using or allowing another person to use any electronic device with recording (audio, photos, video, etc.) or communications capabilities in locker rooms, restrooms, or any other area that could constitute an invasion of any person's reasonable expectation of privacy. Except in an emergency

situation, all such devices should be turned off and put away in all such areas of the buildings.

g. Students who bring a personal electronic device to school are responsible for keeping their device(s) silent during instructional time, or completely turned off and put away to the extent otherwise required or directed.
h. Students using headphones or ear buds are individually responsible for ensuring that they are still adequately able to hear relevant activity (voices, vehicles, announcements, etc.) in their surroundings. The District recommends that at least one ear should be completely clear any time students are moving from one location to another, not including when the student is only a passenger in a vehicle.
i. A student may connect an Internet-ready device with wireless connectivity to the building's "Student/Guest" wireless network in order to use the device for an authorized purpose. A personal unauthorized electronic device shall <u>not</u> be physically connected to any District network other than the "Student/Guest" wireless network.
j. Unless otherwise directed by a District staff member, a student of any age may engage in instructional and limited personal use of a personal electronic device that is connected to the District's "Guest" wireless network if the use (1) occurs outside of the hours of the school's instructional day; (2) does not interfere with any student's education or any school-related activity; (3) does not unduly burden the District's network resources or materially interfere with others' use of the network; and (4) imposes no tangible incremental costs to the District.
k. If a student possesses and uses a personal electronic device that can access a data connection (e.g., 3G/4G) other than a District network, any use of such a device that occurs at school or in connection with a school activity still must be consistent with District rules of conduct for students, including rules regarding the time, place, and manner of such use. The student shall not use the device to access or transfer harmful or inappropriate material, including but not limited to material that is obscene, sexually-explicit, unlawful, threatening, or harassing. These expectations apply even though a device using a non-school data connection is <u>not</u> subject to the District's Internet filtering and related security measures.
l. As an important exception to all rules and directives that might otherwise limit a student's permission to possess and use a personal electronic device, all students at all grade levels may use a device (at any time of day) to contact a responsible adult in any emergency situation that involves an immediate threat to the health or safety of any person. When carrying out school emergency response plans, however, students may be asked to turn off their personal electronic devices so emergency communication networks are not overwhelmed and emergency response efforts are not jeopardized.
m. At all times other than emergencies as identified in the paragraph above, permission to possess and/or use personal electronic devices at school or in any school-supervised setting is subject to further modification or limitation by a teacher, activity supervisor, or any school administrator. When a staff member issues a specific directive or limitation related to the possession or use of any electronic device, students are expected to follow that directive/limitation.
n. Students and parents/guardians are advised that the best way to contact each other during the school day for all non-emergency reasons is through the school office.
o. <u>Additional BYOD Provisions Specific to Students in Grades 4 and Below</u>

- A student in any grade below the 5th grade may not use a personal electronic device during the school day unless the student receives direct permission from a staff member to use the device at that time. A staff member may authorize such use in connection with a specific school-related and school-supervised activity or as a supplement to classroom instruction (e.g., e-readers can be used during classroom reading time).
- When an elementary student has not received permission to use his/her device, the device should be turned off and put away at all times during the school day.

p. Additional BYOD Provisions Specific to Students in Grades 5 through 8

- Personal electronic devices may be used in the classroom or during a student's participation in organized school activities only with the advance approval of the teacher, activity supervisor, or an administrator.
- Students wishing to use a personal electronic device for any instructional or other authorized purpose (including limited personal use) during the school day, but while not in class or while not participating in an organized school activity, must obtain advance approval from a teacher or administrator. A student obtaining such permission shall limit his/her use of the device to the approved time, location, and purpose.

q. Additional BYOD Provisions Specific to High School Students

- Personal electronic devices may be used in the classroom or during a student's participation in organized school activities only with the advance approval of the teacher, activity supervisor, or an administrator.
- Unless otherwise directed by a District staff member, high school students may engage in instructional and/or limited personal use of a personal electronic device when the student is neither attending a class nor participating in an organized school activity, provided that (1) the use does not interfere with and is not likely to disrupt any student's education or any school-related activity; (2) the use does not unduly burden the District's network resources or materially interfere with others' use of the network; and (3) the use imposes no tangible costs to the District.

8. REPORTING STUDENT/PARENT CONCERNS, MISUSE, OR OTHER POSSIBLE VIOLATIONS OF ACCEPTABLE USE.

a. Any time a student feels unsafe, victimized, or in any way uncertain about a situation involving the use of District technology resources by any person, the student (or his/her parent or guardian) should immediately contact a teacher or an administrator.
b. Students are required to report and provide to a teacher or administrator any electronic communication that they receive while using a District-provided email account, or using any District-provided electronic software, program, application or platform if any of the following apply:

- The communication is from an unknown source and either contains inappropriate content, asks the student to respond, or requests the student to reveal personal information;

- The content of the communication is defamatory, discriminatory, threatening, offensive, racist, deceptive, sexually explicit, or obscene;
- The communication represents an attempt to bully, harass, or intimidate another person; or
- The content of the communication represents an attempt to facilitate or encourage any violation of the law or school rules.

c. A student may report to any teacher or to the building principal or any other administrator any concerns about possible violations of the policies, rules, regulations and directives that govern the acceptable, safe, and responsible use of the District's technology-related resources.
d. If a student has a concern that any District technology equipment, network, or system may have a security vulnerability, or that any breach of security may have occurred, the student shall report the issue to a teacher or to the building principal or any other administrator. The student should not demonstrate the potential security problem to anyone other than to the person to whom they report the concern.
e. If a student or parent or guardian has a concern that any content that is available through the Internet is (1) appropriate material that is currently being blocked or filtered, or (2) harmful or inappropriate material that is not being blocked or filtered,

the individual may report that concern to the student's building principal. The District will review the issue and report back to the person making the report.

Adoption Date:

First Reading: **July 9, 2018**
Second Reading: **August 13, 2018**

School District of Platteville
Platteville, Wisconsin